Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide

Version 3.0

July 18, 2007

Prepared For:

Microsoft Corporation
Corporate Headquarters
One Microsoft Way
Redmond, WA 98052-6399

Prepared By:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. This work is licensed under the Creative Commons Attribution-NoDerivs-NonCommercial License (which allows redistribution of the work). To view a copy of this license, visit http://creativecommons.org/licenses/by-nd-nc/1.0/ or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Copyright © 2008 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide

Version 3.0, 7/18/2007

1. INTRODUCTION 1

AUDIENCE ASSUMPTIONS 1

DOCUMENT OVERVIEW 1

CONVENTIONS 2

2. SECURITY ADMINISTRATION 3

OVERVIEW OF SECURITY FUNCTIONALITY 3

ROLES AND PRIVILEGES 5

Role-Based Security 5

WINDOWS SERVER 2003 SECURITY CONFIGURATION 5

System Requirements 6

Hardware 6

Software 7

Evaluated Operating System Software Configuration 9

3. ADMINISTERING WINDOWS SERVER 2003 SECURITY 11

OPERATING ENVIRONMENT 11

Organizational Security Policies 11

Secure Usage Assumptions 11

Connectivity Assumptions 12

Personnel Assumptions 12

Physical Assumptions 12

WINDOWS SERVER 2003 SECURITY MANAGEMENT INTERFACES 13

Security Policy Tools 13

Local Security Settings interface 13

Default Domain Security Settings interface 14

Domain Controller Security Policy interface 14

Group Policy interface 14

Resultant Set of Policies (RSoP) interface 15

Distributed File System (DFS) Management Snap-in 16

Active Directory Federated Services (ADFS) interfaces 16

ADFS Management interface 16

Trust Policy Properties interface 17

My Organization interfaces 18

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Partner Organizations interfaces 19
Windows Server Update Services (WSUS) interface *19*
Account Management Tools *20*
Active Directory Users and Computers 20
Computer Management 20
Active Directory Management *21*
Active Directory Sites and Services 21
Active Directory Domains and Trust 21
System Security Configuration, Maintenance, and Monitoring *22*
Windows Explorer 22
Registry Editor 23
System Services 23
IIS Manager 24
Event Viewer 25
Local Area Connection 25
Disk Quota 25
Backup 26
Error Checking Tool 26
Date/Time Properties 27
Display Properties 27
Configuration Wizards *28*
Active Directory Installation Wizard 28
Delegation of Control Wizard 28
Security Configuration Wizard 28
IP Security Policy Wizard 29
Security Rule Wizard 29
Certificate Export and Import Wizards 30
SECURITY FUNCTIONS 30
Windows Server 2003 Security Policies *32*
Local Security Policy 32
Domain Security Policy 34
Domain Controller Security Policy 35
Site GPO's 36
OU GPO's 38
Account Policies *39*
Configuring Password Policies 40
Configuring Account Lockout Policies 45

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Unlocking a User Account 49
Configuring Kerberos Policies 51
Local Policies *55*
Configuring Audit Policies 55
Best Practices for Auditing 57
Enabling Object Auditing 58
Enabling Auditing on Directory Objects 58
Enabling and editing Audit on Files and Folders 61
Selecting Where to Apply Auditing Entries on Files and Folders 65
Enabling Auditing of IPSec Data Integrity Violations and Replay of TFS Data 66
Enabling and Editing Audit on Registry Keys 66
Selecting Where to Apply Auditing Entries on Registry Keys and Subkeys 69
Configuring User Rights 70
Assigning User Rights and Privileges 73
Configuring Domain-Level User Rights and Privileges 73
Configuring Local User Rights and Privileges 77
Configuring Security Options 79
Configuring ST Requirements through the Group Policies Security Options Interface 81
Prevent Users from Installing Print Drivers 81
Implementing an Authorized Usage Warning 82
Disable Shut Down Without Logging On 83
Set Minimum Session Security for NTLM Security Support Provider (SSP) Based (including secure RPC) Clients and Servers 84
Shut Down System Immediately If Unable to Log Security Audits 85
Configuring Security Target Requirements through the Registry Editor 88
Generate an Audit Event when the Audit Log Reaches a Percent Full Threshold 88
RSoP Snapin *90*
Resultant Set of Policy Snap-in Core Scenarios 90
Logging Mode 91
Planning Mode 91
Using the RSoP Snap-in 92
Using the RSoP from a Domain Controller 96
Creating and Maintaining User and Group Accounts *99*
Computer Accounts 99
Adding and Deleting Computer Accounts 99
Adding a Computer Account to a Group 101
Group Accounts 102

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Group Scope and Group Type 102
Changing Group Scope 103
Group Types 103
Converting between Security and Distribution Groups 104
Creating Group Accounts 104
Adding Group Members 107
Removing Group Members 110
Nesting Groups 111
Deleting a Group 112
User Accounts 113
Creating User Accounts 113
Deleting a User Account 117
Resetting a User Password 117
Modifying Account Properties 121
The Properties interface 122
Configuring Logon Hours 123
Automatically Log Off Users when Logon Time Expires 124
Set an Account Expiration Date 124
Disabling and Enabling User Accounts 125
Data Protection 127
Hardware Data Execution Prevention (DEP) Settings on 64-bit Operating Systems 127
Verify use of hardware DEP 127
Configure use of hardware DEP for 32-bit processes 128
Setting Access Controls on Files, Folders, Shares, and Other System Objects 132
Security Descriptors 133
Copying vs. Moving 133
File Permissions 133
Folder Permissions 134
Selecting where to Apply Permissions 135
Setting or Modifying Permissions 137
How Inheritance affects File and Folder Permissions 139
Shared Folder Permissions 142
Default Share Permissions 143
How Shared Folder Permissions are Applied 144
Guidelines for Shared Folder Permissions 144
Sharing Folders 145
Administrative Shared Folders 145

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Sharing a Folder 146
Assigning Shared Folder Permissions 147
Modifying Shared Folders 150
Combining Shared Folder Permissions and NTFS Permissions 151
Disconnecting a User or Users from a Share or Active Session 152
Active Directory Object Permissions 153
Setting Printer Security Permissions and Printer Shares 156
Delegating Administrative Control 159
Content Indexing Service 163
Accessing Indexing Service 163
Configuring Indexing Service Properties 164
Configuring Indexing Service Usage 165
Controlling System Catalog Directories 166
Querying the System Catalog 167
Scheduled Tasks 169
Adding and managing Scheduled Tasks 169
Using the Scheduled Tasks command-line tool 178
Using the AT scheduler tool 178
Administering IPSec 179
Default IPSec Policy Templates 179
Predefined Filter Lists 180
Predefined Filter Actions 180
Predefined Rules 181
IPSec Policy Templates 181
IPSec Policy Components 183
Configuring IPSec Policies 186
Group Policy 186
Create an IPSec Policy for a Windows Server 2003 Domain 186
Assign an IP Security Policy to a Windows Server 2003 Domain 196
Edit and Existing IP Security Policy 197
IPSec Policy Agent Service 198
Firewalls and IPSec 199
Implementing the Encrypting File System in Windows Server 2003 199
EFS Enhancements in Windows XP and Windows Server 2003 199
Components of EFS 200
Enabling 3DES 201
Changing the Default RSA Key Sizes for Keys Generated for EFS 202

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Maintaining File Confidentiality 202
Encrypting a File or Folder 202
Obtaining EFS Certificates 204
Import EFS Certificates 204
Request an EFS Certificate from a CA within a Domain 207
Granting Local Users Authorization to Open Encrypted Files 209
Granting Domain Users Authorization to Open Encrypted Files 211
Revocation Checking 215
Removing a User's Authorization to Open an Encrypted File 216
Decrypting Files and Folders 217
Data Recovery 217
Data Recovery on Stand-alone Windows Server 2003 218
Data Recovery on Domain Members 224
Copying an Encrypted Folder or File 227
Moving or Renaming an Encrypted Folder or File 228
Deleting an Encrypted Folder or File 228
System Folders and Files 228
Encryption and Local Account Password Resets on Windows Server 2003 228
Backing Up an Encrypted Folder or File 229
Restoring an Encrypted Folder or File 232
Restoring Files to a Different Computer 234
Folder and File Encryption on a Remote Server 239
Remote EFS Operations in a Web Folder Environment 239
Audit Management 240
Viewing the Security Log 240
Configuring the Event Logs 242
Searching for Specific Events 245
Adding another View of an Event Log 246
Per-User Selective Audit 247
Archiving an Event Log 249
Change the Default Event Viewer Log File Location 250
Windows Firewall Configuration and Management 251
Windows Firewall Features 251
Global Configuration Options 252
Connection Specific Configuration Options 252
Operating Modes for Excepted Traffic 253
Startup Security 254

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Incoming Traffic Scoping for IPv4 254
Built-in Support for IPv6 254
Specifying Exempted Traffic by Program File Name 254
Windows Firewall Group Policy Settings 255
Windows Firewall and the Impact to Enterprise Networks 255
Using the Windows Firewall and IPSec 255
Configuring Windows Firewall Settings 256
Configuring Windows Firewall through Domain Group Policy Settings 261
Accessing the Windows Firewall Settings in the Domain Local Policy GPO 262
Specifying Windows Firewall Settings in a Group Policy 264
Automated Configuration of Windows Firewall with SCW 266
SCW 266
Installing the Security Configuration Wizard 267
Accessing the Security Configuration Wizard 268
SCW Command-line Tool 270
IIS 6.0 271
Installing IIS 6.0 272
IIS Manager 275
IIS Web Site Authentication 275
Authentication Based on User Credentials 275
Authentication Based on Requesting Host 278
Trust for Delegation Configuration in Active Directory for IIS Hosts 279
IIS Virtual Directories 283
Configuring SSL on a Web Server or Web Site 285
Request a Server Certificate 285
Install a Server Certificate and Configure SSL 287
Configuring Web Permissions for Web Content 289
Web Service Extensions 292
Internet Printing 294
Installing the Internet Printing Component of IIS 294
Turn on Internet Printing 295
Configure the Authentication Method and Access Control for Internet Printing 296
Connect to a Printer Using a URL 298
WebDAV 301
WebDAV Clients 302
WebDav Integrated Security 302
Installing the WebDAV Publishing Component of IIS 302

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Enable the WebDAV Web Service Extension in IIS Manager 303
Creating WebDAV Publishing Directories 304
Authenticating Clients 306
Controlling Access 306
Configuring Web Permissions 306
Controlling Access with DACLs 307
Protecting Script Code 307
Enabling the WebClient Service 307
Connecting to a WebDAV Directory 308
Remote EFS Operations on File Shares and Web Folders (WebDAV folders) 312
Remote EFS Operations in a Web Folder Environment 312
Remote Encryption of Files on Web Folders 312
Remote Decryption of Files on Web Folders 313
File Copy from a Web Folder 313
IIS 6.0 URL Authorization 313
Sample Script 314
Configuring URL Authorization 316
ASP.NET 2.0 Framework Support Service 330
Configuration Files 330
Accessing the ASP.NET 2.0 MMC Snap-in 331
ASP.NET Configuration Settings – General Tab 332
ASP.NET Configuration Settings – Custom Errors Tab 334
ASP.NET Configuration Settings – Authorization Tab 336
ASP.NET Configuration Settings – Authentication Tab 339
ASP.NET Configuration Settings – Application Tab 340
ASP.NET Configuration Settings – State Management Tab 342
ASP.NET Configuration Settings – Locations Tab 343
Background Intelligent Transfer Service 344
BITS Server Extensions 344
BITS Server Extensions Installation 344
BITS Server Extensions Configuration 346
BITS Server Extensions Configuration Settings 347
Background Intelligent Transfer Service (BITS) Administration Utility 349
Installing BITSAdmin.exe 349
BITS Admin Examples 351
Securing an IIS 6.0 host with the SCW 352
Applying the SCW Security Policy 368

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Implementing Active Directory Federation Services *370*
Understanding Active Directory Federation Services 370
Partner Organizations 371
Account partner 371
Resource partner 372
Federation Trusts 372
ADFS Components and Server Roles 373
Federation server 373
Federation server proxy 373
Web server 374
Types of ADFS-aware Web Applications 374
Claims-aware applications 374
Windows NT token-based applications 375
ADFS Scenarios 375
Federated Web SSO 375
Web SSO 376
Certificates Used by ADFS 377
Token-signing certificates 377
Verification certificates 378
Server authentication certificates 378
Client authentication certificates 378
Cookies Used by ADFS 378
Authentication cookie 378
Account partner cookie 379
Sign-out cookie 379
ADFS Operations 379
Reading the Log Files 379
ADFS Event Logging 380
Event logging on the federation server 380
Event logging on the federation server proxy 381
Event logging on the Web Server 381
ADFS Debug Logging 381
Debug logging on the federation server or federation server proxy 382
Debug logging on the Web Server 382
Web Error Reporting 383
Adding an ADFS-enabled Application 383
Adding an application in a Federated Web SSO scenario 383

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Adding an application in a Web SSO scenario 384
Adding a federation server proxy 385
Administering Windows Server Update Services 385
Security Functionality 386
Logging 386
Management 387
Access the WSUS 3.0 administration interface 387
Managing Windows Server Update Services 388
WSUS 3.0 Synchronizations 388
Managing Updates 390
Managing Updates with WSUS 390
Update Classifications 391
Viewing the Updates 391
Approving the Updates 404
Unapproving Updates 407
Selecting a deadline for updates 408
Approving Updates Automatically 409
Automatically Approving Revisions to Updates and Declining Expired Updates 411
Declining Updates 412
Running WSUS 3.0 in Replica Mode 413
Schedule Update Installations 415
Use Group Policies to configure Automatic Update settings on WSUS 3.0 clients 416
Reports in Windows Server Update Services 3.0 416
Terminology for Update Status 416
Creating Reports 417
Update Reports 418
Computer Status Reports 422
Synchronization Results Report 422
Forests and Domains 424
The Logical Structure of Active Directory 425
Components of the Logical Structure 425
Domains 426
Domains as Containers within a Forest 426
Organizational Units and Objects 427
Organizational Units 427
Objects 428
Forests 428

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Forests as Collections of Domain Containers that Trust Each Other 429
Forest Root domain 430
Domain Trees 430
Child Domains 431
Trust Relationships 431
Managing Domains and Trusts 432
DNS configuration and Active Directory 433
Convert a Windows Server 2003 Server to a Domain Controller for a New Forest 433
Create a New Domain Tree 435
Create a New Child Domain in an Existing Domain Tree 439
Add a Domain Controller to an Existing Domain 440
Raise the Domain Functional Level 442
Remove a Domain 445
Configuring One-way Non-transitive Trusts 446
Smart Card Deployment *448*
Supported Smart Card Reader and Smart Card for the Evaluated Configuration 449
Installing a Smart Card Reader 449
Smart Card Certificate Enrollment 451
Prepare a Certification Authority to Issue Smart Card Certificates 452
Prepare a Smart Card Certificate Enrollment Station 463
Add a Certificate to a Smart Card on Behalf of a User 465
Logging on to a Computer with a Smart Card 468
Changing the Smart Card PIN 469
Distributed File System (DFS) *471*
Key Scenarios 471
DFS Namespaces 472
Namespaces Size Recommendations 472
Security requirements for creating and managing namespaces 472
Installation Requirements 473
Operating system and server requirements 473
Client compatibility for DFS Namespaces 474
DFS Namespace installation and configuration procedures 474
DFS Replication 476
DFS Replication Requirements 476
Active Directory requirements for DFS Replication 476
Operating system requirements for using and managing DFS Replication 476
Security requirements for creating and managing DFS Replication 476

Copyright © 2008 Microsoft Corporation.
All rights reserved.

DFS Replication installation and configuration procedures 477
Routine Operations *488*
Setting IP Address Information and Host Security 488
Joining a Computer to a Domain or Workgroup 491
Remove a Computer from a Domain 492
Disable Unnecessary System Services on Domain Computers 493
Disable Unnecessary System Services Locally 494
Locking and Unlocking a User Desktop 494
Managing Disk Quotas 496
Setting Disk Quotas 497
Determining the Status of Disk Quotas 499
Monitor Disk Quotas 499
Exceeding Disk Quota Limits 500
Active Directory Sites and Services *501*
To Delegate Control 505
Active Directory Replication 506
Active Directory Replication Model 506
Replication Model Components 507
Replication Latency 507
State-based vs. log-based Replication 508
Multimaster vs. Single-master Replication 508
Pull vs. Push Replication 508
Active Directory Replication Dependencies 509
Active Directory Replication Topology 509
Replication Within and Between Sites 509
Technologies Related to Active Directory Replication Topology 510
Active Directory Replication Topology Dependencies 510
How replication Works 511
Transferring Replication Data 511
Preventing Unnecessary Replication 511
Resolving Conflicting Changes 511
Improving Replication Efficiency 511
Replication Within a Site 512
Building the Intra-site Replication Topology 512
Determining when Intra-site Replication Occurs 512
Replication between Sites 512
Building the Inter-site Replication Topology 512

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Determining when Inter-site Replication Occurs 513
When to Establish a Single or Separate Sites 513
Why Bandwidth is Important 513
When to Establish a Single Site 513
When to Establish Multiple Sites 514
Managing Replication 514
Creating and Deleting Site Links 514
Adding a Site to a Site Link 516
Creating and Deleting a Site Link Bridge 516
Enabling and Disabling a Site Link Bridge 517
Configuring Site Link Replication Availability 518
Configuring Site Link Cost 520
Configuring Site Link Replication Frequency 520
Forcing Replication over a Connection 521
Manually Adding Connections 521
Protection of TSF 522
Set the Date and Time 522
Execute Diagnostic Tests – Error Checking Tool 523
Defining and Managing Security Templates 524
Starting Security Templates 525
Customizing a Predefined Security Template 525
Defining a Security Template 525
Deleting a Security Template 525
Refreshing the Security Template List 526
Setting a Description for a Security Template 526
Applying a Security Template to a Local Computer 526
SECURITY-RELEVANT EVENTS 527
Audit Trail Overflow 527
Review Audit Trails for Suspected Malicious or Illicit Activity 527
User Account is Disabled Due to Exceeded Limit of Unsuccessful Login Attempts 528
Temporary User Accounts are Required (such as for contractor support) 528
Security-Relevant Service Pack or Hot Fix Updates are Available 529
User Joins a Different Part of the Organization, Requiring Access Changes 530
User Leaves Organization 530
User Forgets Password 531
Recovery of User Encrypted Files 531
Incorrect Time 532

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Quota Limit Reached *533*
It is Necessary to Revoke a User's Access to Objects and/or to the User's Privileges *533*
Access to an ADFS-enabled Web Application Must be Revoked from a Current User *534*

4. EXTERNAL SECURITY MEASURES 535

5. ACRONYMS 536

6. REFERENCES 541

APPENDIX A – WINDOWS SERVER 2003 CERTIFICATE SERVER SECURITY CONFIGURATION GUIDE A-1

GENERAL HARDWARE AND OPERATING ENVIRONMENT CONFIGURATION A-1
SOFTWARE CONFIGURATION A-1
CA ROLES AVAILABLE IN MICROSOFT WINDOWS SERVER 2003 ENTERPRISE EDITION A-1
CERTIFICATE SERVER INSTALLATION A-3
Preparing for Installation *A-3*
Windows Server 2003 Certificate Server Installation Process *A-4*
Installation of the Hardware Security Module A-4
HSM Installation Procedures A-4
Create the nCipher Security World A-8
Installation of the Windows Server 2003 Certificate Server A-13
Windows Server 2003 Certificate Server Installation A-13
Complete the installation of a subordinate CA associated with an offline parent CA A-20
Install a CRL from a parent CA A-20
Install the parent CAs certificate A-23
Install the subordinate CAs certificate A-26
Add CRL Distribution Points and Authority Information Access Extensions to a Root CA A-27
Renewing the CA's Certificate A-28
Trusted Root Certification Authorities Group Policy Settings A-31
Adjusting the Clock Skew Registry Settings A-33
CONFIGURATION OF CERTIFICATE SERVER MANAGEMENT ROLES A-35
Define Authorized Accounts for CA Management Roles *A-35*
Assign CA Administrator Role *A-37*
Assign Certificate Manager Role *A-38*
Assign CA Backup Operator Role *A-40*
Assign CA Auditor Role *A-40*
Set Administrative Tools Menu for CA Management Roles A-44
Remove Default Accounts from CA Management Roles *A-44*
Set Template Permissions and Ownership *A-45*

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Role Separation *A-52*
Enable Role Separation A-52
Allow the CA Administrator to Set CA Audit Event Categories A-53
SECURE CONFIGURATION OF THE CERTIFICATE SERVER A-55
CA Audit Configuration *A-55*
Configuration of CA Audit Parameters A-55
System Services *A-58*
Disable Unnecessary System Services A-59
Securing the Certification Authority's Database and Logs *A-60*
File and Folder Permissions A-60
Set Permissions on the CA Database and Logs through Windows Explorer A-61
Auditing of CA Database and Log Access A-61
Set Auditing on CA Files and Folders through Windows Explorer A-62
REGISTRY AUDIT SETTINGS A-62
Set Auditing on CA Registry Keys A-63

APPENDIX B - WINDOWS SERVER 2003 CERTIFICATE SERVER ADMINISTRATOR'S GUIDE B-1
AUDIENCE ASSUMPTIONS B-1
PUBLIC KEY INFRASTRUCTURE CONCEPTS B-1
Online PKI Planning Resources *B-1*
Additional PKI Book Resources for Planning *B-2*
OVERVIEW OF SECURITY FUNCTIONS B-2
CA MANAGEMENT ROLES AND ASSOCIATED PRIVILEGES B-4
NETWORK-LEVEL IT ENVIRONMENT B-4
Networked Systems Supported by the Certificate Server *B-5*
Networked Systems Supporting the Certificate Server *B-5*
ADMINISTERING WINDOWS SERVER 2003 CERTIFICATE SERVER SECURITY B-6
Certificate Server Security Management Interfaces *B-6*
Microsoft Management Consoles B-6
Certification Authority MMC Snap-in B-6
Certificates MMC Snap-in B-7
Certificate Templates MMC Snap-in B-7
Configuration Wizards B-7
Command-line Tools B-8
Security Functions *B-8*
Role-Based Certification Authority Management B-11
Assignment of Certification Authority Management Roles B-11
Removing Role Assignments B-11

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Administering a Certification Authority B-11
Starting and stopping certificate services B-12
Certification Authority backup and recovery B-12
Configuring auditing of CA administrative actions B-19
Renewing CA Certificates B-25
Managing Certificate Revocation B-34
Managing Certificate Requests B-43
Certificate Profile Management B-45
Modification of Certificate Fields B-58
CA Key Management B-77
Changing policy settings on the CA B-77
Security-Relevant Events B-81
Compromise of Private Key for User, Service or System B-81
User Leaves Organization B-81
Audit Certification Authority Management Activities B-82
User Must Be Removed from a CA Management Role B-82
A New User Must Be Granted a CA Management Role B-83

Copyright © 2008 Microsoft Corporation.
All rights reserved.

1. Introduction

Welcome to the *Microsoft Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0*. This document provides sufficient guidance to allow an administrator to securely operate Windows Server 2003 in accordance with the requirements stated in the *Microsoft Windows 2003, XP Professional and XP Embedded Security Target*.

The *Microsoft Windows 2003, XP Professional and XP Embedded Security Target*, defines the requirements for Version 3.0 of the Windows Server 2003 and XP Professional Common Criteria Evaluation and is henceforth referred to as the Windows 2003/XP V3 ST. The Windows 2003/XP V3 ST provides a set of security requirements taken from the CC for Information Technology (IT) Security Evaluation. Windows Server 2003 product was evaluated against the Windows 2003/XP V3 ST and found to satisfy the ST requirements.

This document is targeted at the administrator and provides a description of how to perform the administrative security functions needed to securely operate Windows Server 2003 in accordance with the ST requirements.

Audience Assumptions

This document assumes the administrator is familiar with the security features of the Windows Server 2003 product. To administer a Windows Server 2003 computer or system, one should be familiar with the product documentation for the operating system such as the Windows Server 2003 Deployment Kit and the Windows Server 2003 Technical Reference (formerly the Windows Server Resource Kit). Together these documents provide a complete set of deployment and technical reference information for the Windows Server 2003 family of operating systems (OSes).

Document Overview

This document has the following chapters:

Chapter 1, "Introduction," introduces the purpose and structure of the document and the assumptions of the audience.

Chapter 2, "Security Administration," describes the Evaluated Configuration and provides an overview of the security functionality.

Chapter 3, "Administering Windows Server 2003 in a Secure Manner," provides a description of each of the security functions that must be performed by the administrator to securely operate the system in accordance with the requirements stated in the ST.

Chapter 4, "External Security Measures," describes any measures that should be addressed by the Windows Server 2003 environment which require the administrator's attention.

Chapter 5, "Acronyms"

Chapter 6, "References"

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Conventions

Throughout the document, the following conventions are followed:

Warnings: Cautions administrators should take to ensure the system is secure. Warnings are identified with the bolded word Warning (e.g., "**Warning**").

Note: Text that is important for the administrator to take notice of is identified with a bolded word Note (e.g., **Note**).

Evaluated Configuration: Refers to the configuration of Windows Server 2003 that was evaluated and determined to meet the Windows 2003/XP V3 ST.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

2. Security Administration

This section provides an overview of administrating Windows Server 2003 securely by summarizing the following areas:

- Windows Server 2003 Security Functionality
- Roles and Privileges
- Windows Server 2003 Evaluated Configuration

This section lays the foundation for understanding the guidance provided in Chapter 3.

Overview of Security Functionality

This subsection provides an overview of the evaluated functions of the Windows Server 2003 operating system. Additionally, this subsection summarizes the Windows Server 2003 administrative interfaces available to the administrator to securely manage the system.

The security functions provided by Windows Server 2003 are summarized below:

- **Security Audit** – Windows Server 2003 provides the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated, computer where the event occurred, and other event specific data. Authorized administrators can review audit logs. In addition to audit data, the Windows Server Update Services creates extensive logging information. This information is stored and protected in the TOE file system.
- **Identification and Authentication** – Windows Server 2003 requires each user to be identified and authenticated prior to performing any functions. An interactive user invokes a trusted path in order to protect the user's identification and authentication information for the user's primary user account. In addition to participating in an Active Directory enabled domain environment, which provides a network database for domain user accounts, Windows Server 2003 maintains a database of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows Server 2003 includes a set of account policy functions that provide the ability to define minimum password length, number of failed logon attempts, duration of lockout, and password age.
- **Security Management** – Windows Server 2003 includes a number of functions to manage policy implementation. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.
- **User Data Protection** – Windows Server 2003 protects user data by enforcing several access control policies (DAC, WEBUSER, web content provider access control, and Indexing Service access control) and several information flow policies (IPSec filter information flow control, Connection Firewall, and RPC over HTTP); and, object and subject residual information protection. Windows Server 2003 uses access control methods to allow or deny access to objects, such as files, directory entries, printers, and web content. Windows Server 2003 uses information flow control methods to control the flow of IP traffic. It authorizes access to these resource objects through the use of unique Security Descriptors (SDs) (which are sets of information identifying users and their specific access to resource objects), web permissions, IP filters, and port mapping rules. Windows Server 2003 also protects user data by ensuring that resources exported to user-mode processes do not have any residual information.

  Windows Server 2003 R2 with SP2 includes Active Directory Federation Services (ADFS) as a separate, installable component. ADFS is provided to support single sign-on across realms in Web resource access scenarios. Authentication is performed when a client attempts to access a Web

Copyright © 2008 Microsoft Corporation.

All rights reserved.

resource that is ADFS-enabled. The first time the client's request to access the resource is received, the client does not possess a signed security token for accessing the Web application. Therefore, the resource realm re-directs the client request to the client's Federation Service to perform authentication. The federation server hosted in the realm that contains the user's account performs authentication using Active Directory and generates a signed security token. The signed security token is then embedded in a cookie that the client uses when requesting Web services from the resource realm. The ADFS agent on the Web server implants its own discretionary access control (DAC) mechanism. ADFS supports the User Data Protection security function by using the identity information in the signed token to determine access to the Web content following the same rules as those defined for other controlled Web content.

- **Cryptographic Protection** - Windows Server 2003 provides additional protection of data through the use of data encryption mechanisms. These mechanisms only allow authorized users access to encrypted data.
- **Protection of Target of Evaluation (TOE) Security Functions** – Windows 2003/XP provides a number of features to ensure the protection of TOE security functions. Windows 2003/XP protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPSec and ISAKMP. The XP portion of the TSF provides the ability to restore some previously archive TSF data. Windows 2003/XP provides a Windows Server Update Services that allows authorized administrators the ability to manage software updates and control the propagation of updates to individual machines of the TOE. Windows 2003/XP ensures process isolation security for all processes through private virtual address spaces, execution context and security context. The Windows 2003/XP data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory.
- **Resource Utilization** – Windows Server 2003 can limit the amount of disk space that can be used by an identified user or group on a specific disk volume. Each volume has a set of properties that can be changed only by a member of the administrator group. These properties allow an authorized administrator to enable quota management, specify quota thresholds, and select actions when quotas are exceeded.
- **TOE Access** – Windows 2003/XP provides the ability for a user to lock their session immediately or after a defined interval. It constantly monitors the mouse and keyboard for activity and locks the workstation after a set period of inactivity. Windows 2003/XP allows an authorized administrator to configure the system to display a logon banner before the logon dialogue. Windows 2003/XP provides the ASP.NET framework for creating web-based application. Within the ASP framework are several built-in security features such as session timeout and maximum permitted concurrent sessions
- **Web Server Security Functions** - Windows Server 2003 Internet Information Services (IIS) 6.0 supports the following Web server security functions:
  - **Uniform Resource Locator (URL)-Based authorization** - This authorization mechanism enables businesses to control access to applications exposed through the Web by restricting user access to URLs. For example, one user may be restricted from access to certain applications, whereas another user can be allowed to execute other applications.
  - **Web Site Permissions** - Web Site permissions are not meant to be used in place of New Technology File System (NTFS) permissions. Instead, they are used with NTFS permissions to strengthen the security of specific Web site content maintained by the IIS version 6.0 web server of the Windows Server 2003 TOE. An authorized user can configure web site's access permissions for specific sites, directories, and files. Unlike NTFS permissions, Web site permissions affect everyone who tries to access the configured Web sites. If Web permissions conflict with NTFS permissions for a directory or file, the more restrictive settings are applied.
  - **WebDAV Redirector** - Web Distributed Authoring and Versioning (WebDAV) redirector allows files stored in web folders to be encrypted with Encrypting File Service (EFS). When a client maps a drive to a WebDAV access point on a remote server, files may be encrypted locally on the client and then transmitted as a raw encrypted file to the WebDAV server using an HyperText

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Transfer Protocol HTTP "PUT" command. Similarly, encrypted files downloaded to a client are transmitted as raw encrypted files using an HTTP "GET" command and decrypted locally.

Roles and Privileges

The notion of roles within the TOE is generally realized by assigning group accounts and privileges to a given user account. Whenever that user account is used to logon, the user will be assuming the role that corresponds with the combination of groups and privileges that it holds. While additional roles could be defined, this ST defines two logical roles: the *authorized administrator role* and the *authorized user role*.

Role-Based Security

Roles are categories of users that have been defined for the purpose of determining access permissions and privileges to system and account resources. Roles are defined by assigning privileges to a group, or by using one of the predefined groups in Windows Server 2003. Users are then assigned to the appropriate groups in order to grant them the predefined roles access. Users must be assigned to the roles that correctly represent their relationship to the data and resources they are authorized to access throughout the network. When a user is no longer authorized the privileges defined by a role, the administrator can remove the user from the group account(s) that grant those privileges.

The security-relevant functions of the authorized administrator role include those that:

- Are assigned one of the security-relevant privileges (e.g., Take Ownership privilege) or is made a member of one of the several pre-defined administrative groups (e.g., Administrators and Backup Operators local group).
- Define and change the user security characteristics and those of the system security data (e.g., user identifier, user's group identifiers, user/group security restrictions).
- Define and change the system's security characteristics.
- Ensure the enforcement of the system security policy.
- Perform audit functions (e.g., determine what events should be audited, manage the audit trail, analyze the audit trail, and produce audit reports).
- Satisfy the life-cycle assurance requirements of correct implementation and operation.

Any user that can successfully logon and **is not** in an authorized administrator role (as defined above) is considered to be in an authorized user role. Authorized users log on to the network through an account that provides sufficient access to use the resources of the network for business purposes. An authorized user cannot, for example manage network resources, create, modify, or delete accounts, or manage security policies for domain groups. If authorized, a user can assume an administrator role by logging on through a user account that has either been explicitly assigned administrative privileges or belongs to a group that provides the required administrative privileges.

Appendices C and D of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* fully identify all security-related privileges and administrative groups respectively, and provide advice on how and when to assign them to user accounts.

Windows Server 2003 Security Configuration

The primary focus of this subsection is to describe the concept of an "Evaluated Configuration." This subsection does NOT give instruction of how to install and configure the Windows Server 2003 operating system to be in conformance with the Evaluated Configuration. Such instruction is provided in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*. This subsection introduces the

Copyright © 2008 Microsoft Corporation.

All rights reserved.

notion of an "Evaluated Configuration" so the administrator is aware of potential consequences if the system is not properly configured, and specifies the hardware and software requirements.

Note: In using this document, administrators must ensure that the required Evaluated Configuration security settings defined in the Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0 are not altered as a result of day-to-day maintenance operations.

The TOE includes a homogenous set of Windows Server 2003 systems that can be connected via their network interfaces and may be organized into domains. A domain is a logical collection of Windows Server 2003 and Windows XP Professional systems that allows the administration and application of a common security policy and the use of a common accounts database for all systems within the domain. Single and multiple domain configurations can be configured and managed through the use of Windows Server 2003 Domain Controllers. In a multiple-domain configuration, the TOE supports implicit and explicit trust relationships between domains. Domains use established trust relationships to share account information and validate the rights and permissions of users. A user with one account in one domain can be granted access to resources on any server or workstation on the network. Domains can have one-way or two-way trust relationships. Each domain must include at least one designated server known as a Domain Controller to manage the domain.

Warning: Applying the security settings provided in this guide on Windows domains that are not a homogenous set of Windows Server 2003 and Windows XP systems may introduce compatibility issues with down-level Windows platforms.

Each Windows Server 2003 system, whether it is a Domain Controller, a member server, or a standalone server, is part of the TOE and provides a subset of the TSFs. The TSF for Windows Server 2003 can consist of the security functions from a single system (in the case of a standalone system) or the collection of security functions from an entire network of systems (in the case of domain configurations).

Windows Server 2003 SP2 with the Windows Server 2003 R2 software update (Windows Server 2003 R2 SP2), includes Active Directory Federation Services (ADFS) as a separate, installable component. ADFS enables single sign-on (SSO) technologies for authenticating a user to multiple Web applications over the life of a single online session through distributed identification, authentication, and authorization across organizational and platform boundaries. ADFS supports the Identification and Authentication security function by offering the ability to maintain a user attribute database containing user account attributes, including the following.

- User identifier
- Group memberships
- Authentication data
- Security-relevant roles
- Cryptographically signed ADFS security tokens (which may be based on X.509v3 public key certificate, Kerberos, or SAML)

System Requirements

This subsection describes the minimum system requirements for the Evaluated Configuration.

Hardware

Windows 2003 Server Standard Edition supports up to four (4) GigaBytes (GB) of Random Access Memory (RAM) and up to four symmetric multiprocessors. Windows Server 2003 Enterprise Edition takes advantage of larger amounts of memory to improve performance and handle the most demanding applications, with support for up to 32 GB of RAM for x86-based computers and 64 GB of RAM for

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Itanium-based or x64-based computers. It supports up to eight (8) symmetric multiprocessors. Windows Server 2003 Datacenter Edition supports 64 GB of RAM for x86-based computers and 512 GB of RAM for Itanium-based or x64-based computers. It supports a maximum of 64 symmetric multiprocessors.

For the TOE, any of the devices listed below may be attached.

- Display Monitor;
- Keyboard;
- Mouse;
- Floppy Disk Drive;
- Compact Disk (CD)-Read Only Memory (ROM) Drive;
- Fixed Disk Drives;
- Printer;
- Audio Adapter;
- Network Adapter; and
- Smart card reader.

The TOE does not include any physical network components between network adapters of a connection. The ST assumes that any network connections, equipment, and cables are appropriately protected in the TOE security environment.

Software

Windows Server 2003 is an operating system that supports a variety of server configurations (e.g., application server, file server). The TOE includes three product variants of Windows Server 2003: Standard, Enterprise, and Datacenter Editions. Windows Server 2003 additionally provides Domain Controller features including the Active Directory (AD) and Kerberos Key Distribution Center (KDC). Windows Server 2003 in the TOE can also be configured to provide IIS version 6.0, Certificate Server, File Replication, Directory Replication, Domain Naming System (DNS), Dynamic Host Configuration Protocol (DHCP), Distributed File System (DFS) service, Removable Storage Manager, and Virtual Disk Service. Otherwise, all three variants include the same security features. The primary differences between the three variants included in the TOE are explained in the table below. Microsoft offers two other variants that are not included in the TOE; Windows Server 2003, Web Edition and Windows Small Business Server 2003.

Table 2-1 Windows Server 2003 Operating System Product Descriptions

Product	Description
Windows Server 2003, Standard Edition	Windows Server 2003, Standard Edition, is designed for departmental and standard workloads and delivers the following benefits: ▪ Support for file and printer sharing. ▪ More secure Internet connectivity (as compared to Windows 2000 Server). ▪ Centralized desktop application deployment. ▪ Support for 64-bit computing platforms. For more information about the 32-bit version, see the Windows Server 2003, Standard Edition, Overview. For more information about the 64-bit version, see Benefits of Microsoft Windows x64 Editions.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Product	Description
Windows Server 2003, Enterprise Edition	Built for mission-critical server workloads, Windows Server 2003, Enterprise Edition, is the platform of choice for applications, Web services, and infrastructure. Delivering high reliability, performance, and superior business value, Windows Server 2003, Enterprise Edition provides these benefits: ▪ A full-function server operating system that supports up to eight (8) processors. ▪ Enterprise-class features, such as eight-node clustering and support for up to 32 GB of memory.[1] ▪ Support for Intel Itanium-based computers, AMD Opteron processors, or Intel Xeon processors. ▪ Support for 64-bit computing platforms capable of supporting eight (8) processors and 64 GB of RAM with the 64-bit version. For more information about the 32-bit version, see the Windows Server 2003, Enterprise Edition, Overview. For more information about the 64-bit versions, see Benefits of Microsoft Windows x64 Editions and Windows Server 2003 Enterprise Edition for Itanium-based Systems.
Windows Server 2003, Datacenter Edition	Windows Server 2003, Datacenter Edition, is built for the highest levels of scalability and reliability. Only this platform offers the Datacenter High Availability Program of support and services. Benefits of Windows Server 2003, Datacenter Edition, include: ▪ The most powerful and functional server operating system offered. ▪ Support for up to 32-way SMP and 64 GB of RAM with the 32-bit version[2]. ▪ Support for up to 128-way machines with individual partitions of up to 64 processors and 512 GB of RAM with the 64-bit version (the x64version is included in the Evaluated Configuration). ▪ Both 8-node clustering and load balancing services as standard features[3]. ▪ Windows System Resource Manager[4] to facilitate consolidation and system management. For more information about the 32-bit version, see the Windows Server 2003, Datacenter Edition, Overview. For more information about the 64-bit version, see Windows Server 2003, Datacenter Edition for 64-Bit Itanium-based systems and Benefits of Microsoft Windows x64 Editions. The 64-bit Itanium version of Windows Server 2003, Datacenter Edition is not included in the current TOE

The security features addressed by the Windows 2003/XP V3 ST are those provided by Windows Server 2003 as a distributed OS. Microsoft provides several Windows Server 2003 software applications that are considered outside the scope of the defined TOE and not part of the Evaluated Configuration. Services

[1] This feature is not included in the TOE.

[2] The 32-bit version of Windows Server 2003, Datacenter Edition is not included in the TOE.

[3] This feature is not included in the TOE.

[4] The Windows System Resource Manager is not included in the current TOE.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

outside this evaluation include: e-mail services; Terminal Services; Microsoft Message Queue; Right Management Service; and Windows SharePoint Service.

Software applications that are included as required components of the defined TOE, include Active Directory Federated Services (ADFS) and Windows Server Update Services (WSUS) 3.0 and all their supporting architecture components. For more information on ADFS, see Implementing Active Directory Federation Services later in this guide. For more information on WSUS 3.0, see Implementing Windows Server Update Services later in this guide.

Evaluated Operating System Software Configuration

The Evaluated Configuration of Windows Server 2003 includes Windows Server 2003: Standard, Enterprise, and Datacenter Editions configured in any one of the roles shown in the table below and in accordance with the installation and configuration instructions provided in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*. For further information regarding the specific security requirements met by Windows Server 2003, see the Windows 2003/XP V3 ST.

Table 2-2 Windows Server 2003 Roles

Product	Role
Microsoft Windows Server 2003, Standard Edition (32-bit and 64-bit versions)	Domain Controller Domain Member Server Workgroup Member Server Stand-Alone
Microsoft Windows Server 2003, Enterprise Edition (32-bit and 64-bit versions)	Domain Controller Domain Member Server Workgroup Member Server Stand-Alone
Microsoft Windows Server 2003, Datacenter Edition (64-bit version (x64 only))	Domain Controller Domain Member Server Workgroup Member Server Stand-Alone

It is important to understand the difference between a domain and a workgroup environment. The main difference been a domain and a workgroup is that workgroup environments use decentralized administration. This means that every computer must be administrated independently of the others. Domains use centralized administration, in which administrators can create one domain account and assign permissions to all resources within the domain to that one central user or group of users. Centralized administration requires less administration time and provides a more secure environment. In general, workgroup configurations are used in very small environments that have few security concerns. Larger environments and environments that must have tight security on data should use a domain configuration. Basic definitions are provided below.

- **Domain**. A collection of computers defined by the administrator of a Microsoft Windows network that share a common directory database. A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has its own security policies and security relationships with other domains and represents a single security boundary of a Windows computer network from the user account database and Kerberos KDC perspective.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Workgroup**. A logical grouping of networked computers that share resources, such as files and printers. A workgroup is sometimes referred to as a peer-to-peer network because all computers in the workgroup can share resources as equals, without a dedicated server. Each Windows Server 2003 computer in a workgroup maintains its own local security database, which contains a list of user accounts and resource security information specific to that computer.
- **Domain Controller**. For a Windows Server 2003 domain, the Windows Server 2003 server that authenticates domain logons and maintains the security policy and the security accounts master database for a domain. Domain Controllers manage user access to a network, which includes logging on, authentication, and access to the directory and shared resources. Two or more Domain Controllers within a domain also have evaluated replication mechanisms to ensure data replication consistency of their database contents.
- **Workgroup Member**. A Windows Server 2003 computer that is a member of a Windows workgroup (the workgroup may include both Windows XP Professional and Window Server 2003 computers), formed as a logical grouping of networked computers for the purpose of sharing resources.
- **Domain Member**. A Windows XP Professional or a Windows Server 2003 computer that is a member of a Window Server 2003 domain environment.
- **Stand-Alone**. Windows Server 2003 computer that is not connected to any network as either a domain or workgroup member.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. Administering Windows Server 2003 Security

This section describes how to operate Windows Server 2003 according to the TOE security policy in an IT environment that is consistent with the one described in the Windows 2003/XP V3 ST. It describes effective security practices for administering Windows Server 2003 in a secure manner. This includes properly setting up user accounts, reviewing audit records, enforcing periodic password changes, etc.

Operating Environment

The security environment of the Evaluated Configuration of Windows Server 2003 is described in the Windows 2003/XP V3 ST and identifies the potential threats against Windows Server 2003, the organizational security policies, and the usage assumptions as they relate to Windows Server 2003. The assumptions and policies are primarily derived from the Controlled Access Protection Profile (CAPP), while the threats were introduced in the Windows 2003/XP V3 ST to better represent specific threats addressed by Windows Server 2003. The administrator should ensure that the environment meets the organizational policies and assumptions. They are repeated below from the Windows 2003/XP V3 ST.

Organizational Security Policies

Table 3-1 describes organizational security policies that are addressed by Windows Server 2003.

Table 3-1 Organizational Security Policies

Security Policy	Description	PP Source
P.ACCOUNTABILITY	The users of the system shall be held accountable for their actions within the system.	CAPP
P.AUTHORIZED_USERS	Only those users who have been authorized access to information within the system may access the system.	CAPP
P.NEED_TO_KNOW	The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a "need to know" for that information.	CAPP
P.AUTHORIZATION	The system must have the ability to limit the extent of each user's authorizations.	
P-ADD-IPSec	The system must have the ability to protect system data in transmission between distributed parts of the protected system	
P.WARN	The system must have the ability to warn users regarding the unauthorized use of the system.	

Secure Usage Assumptions

This subsection describes the security aspects of the environment in which the Windows Server 2003 operating system is to be used. This includes assumptions about the connectivity, personnel, and physical aspects of the environment.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Windows Server 2003 is assured to provide effective security measures in the defined environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with the user and administrator guidance.

Connectivity Assumptions

Windows Server 2003 is a distributed system connected via network media. It is assumed that the following connectivity conditions will exist.

Table 3-2 Connectivity Assumptions

Assumption	Description	PP Source
A.CONNECT	All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.	CAPP
A.PEER	Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address the need to trust external systems or the communications links to such systems.	CAPP

Personnel Assumptions

It is assumed that the following personnel conditions will exist.

Table 3-3 Personnel Assumptions

Assumption	Description	PP Source
A.COOP	Authorized users possess the necessary authorization to access at least some of the information management by the TOE and are expected to act in a cooperating manner in a benign environment.	CAPP
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	CAPP
A.NO_EVIL_ADM	The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.	CAPP

Physical Assumptions

Windows Server 2003 is intended for application in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Table 3-4 Physical Assumptions

Assumption	Description	PP Source
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	CAPP
A.PROTECT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	CAPP

Windows Server 2003 Security Management Interfaces

This subsection provides a brief description of the security management interfaces used to modify and apply security configuration settings, manage user and computer accounts, manage domain resources, and monitor events on Windows Server 2003 operating environments.

Security Policy Tools

This document discusses several tools that are used to apply and manage security policy settings locally on a computer or across the domain.

Local Security Settings interface

The **Local Security Settings** interface is used to implement Local Security Policy settings on a computer. These settings include the Password policy, Account Lockout policy, Audit policy, IPSec policy, user rights assignments, recovery agents for encrypted data, and other security options. The Local Security Settings interface is primarily used for stand-alone computers or to apply specific security settings to a domain member that does not receive a full set of policies from the domain. Within an Active Directory managed network, the Local Security Policy applied by the Local Security Settings interface has the least precedence with respect to policy. Therefore, if the computer is a member of a domain, the settings within the Local Security Settings interface may be overridden by policies received from the domain.

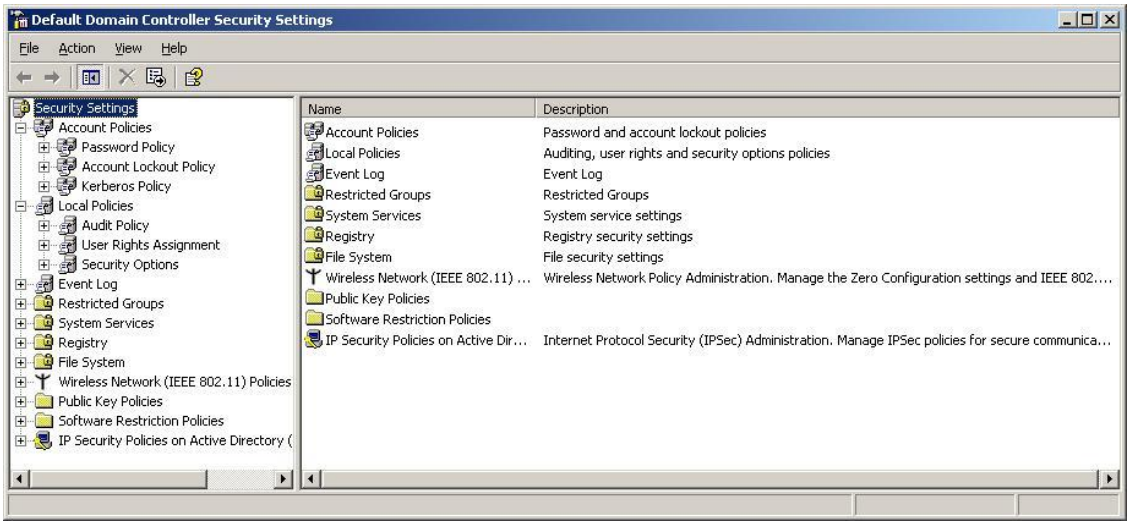
Note: On a Windows Server 2003 Domain Controller, the Local Security Settings interface is not used. Security policies on a Domain Controller are applied by the Domain Security Policy and the Domain Controller Security Policy.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

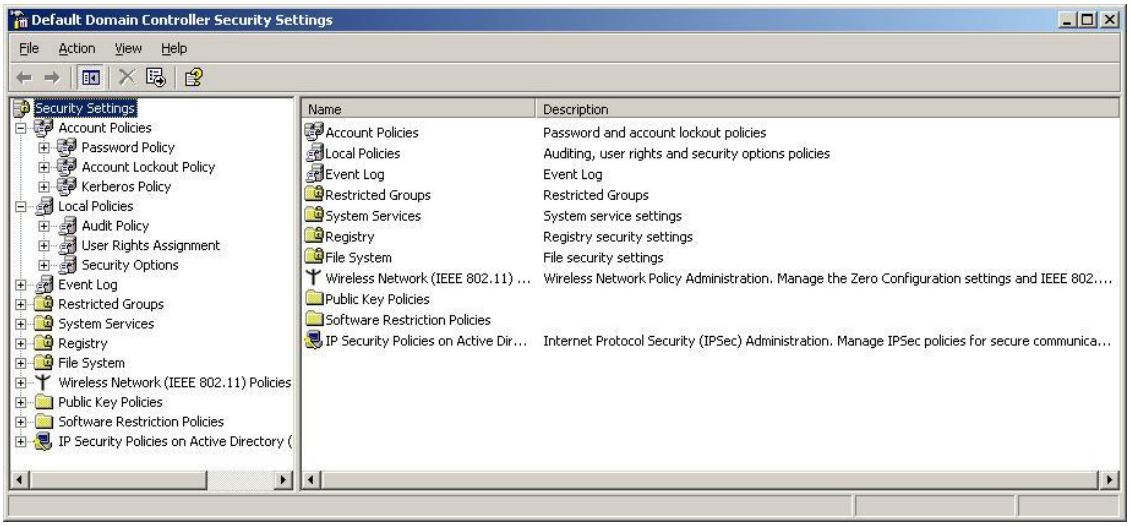
Default Domain Security Settings interface

A **Default Domain Security Settings** Interface is used to set and propagate Domain Security Policy requirements for all computers within a domain. The Default Domain Security Policy overrides Local Security Policy settings for all computers within the Domain.



Domain Controller Security Policy interface

A **Domain Controller Security Settings** Interface is used to set and propagate security requirements for Domain Controllers. The Domain Controller Security Policy applies strictly to all Domain Controllers within the applicable Domain and takes precedence over the Domain Security Policy.

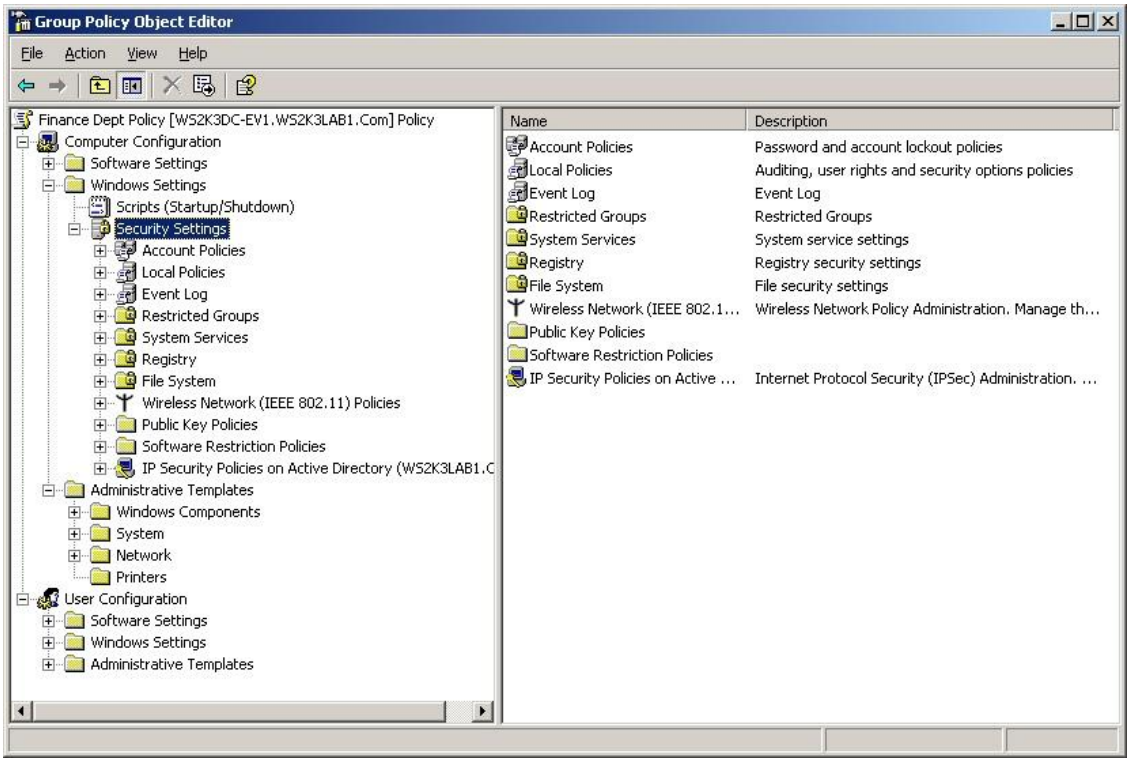


Group Policy interface

The group policy management functions allow an authorized administrator to define accounts, user right assignments, and machine/computer security settings, etc. for a group of computers or accounts within a domain. The group policies effectively modify the policies (e.g., machine security settings, and user rights policy) defined for the corresponding systems or users.

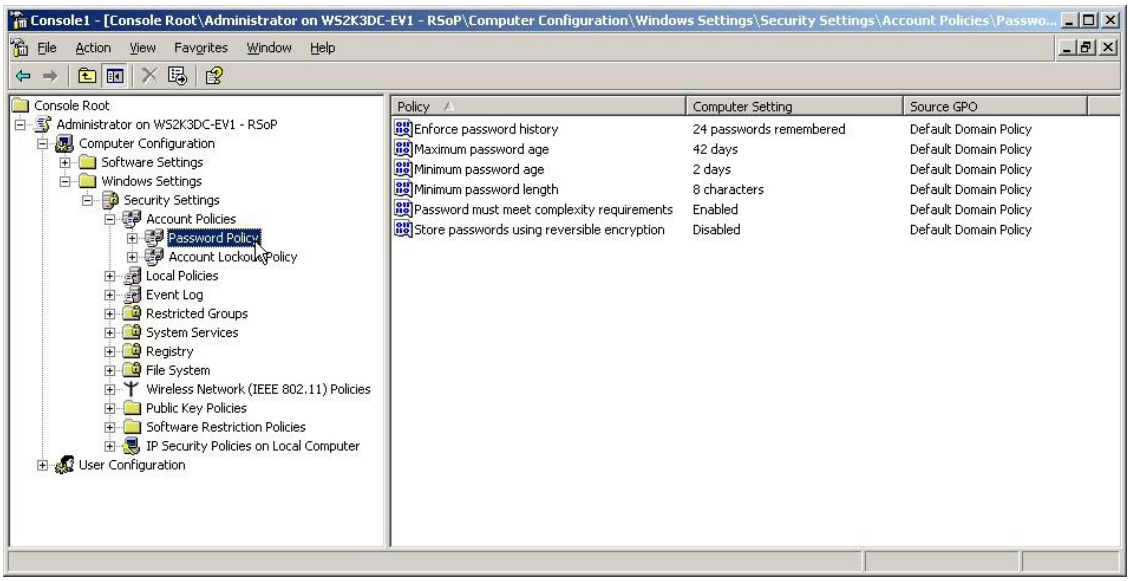
Copyright © 2008 Microsoft Corporation.

All rights reserved.



Resultant Set of Policies (RSoP) interface

Resultant Set of Policy (RSoP) is an addition to Group Policy used for managing and troubleshooting policies. RSoP is a query engine that polls existing policies and planned policies, and then reports the results of those queries. When policies are applied on multiple levels (for example, site, domain, Domain Controller, and organizational unit), the results can conflict. RSoP can help administrators determine a set of applied policies and their precedence (the order in which policies are applied).

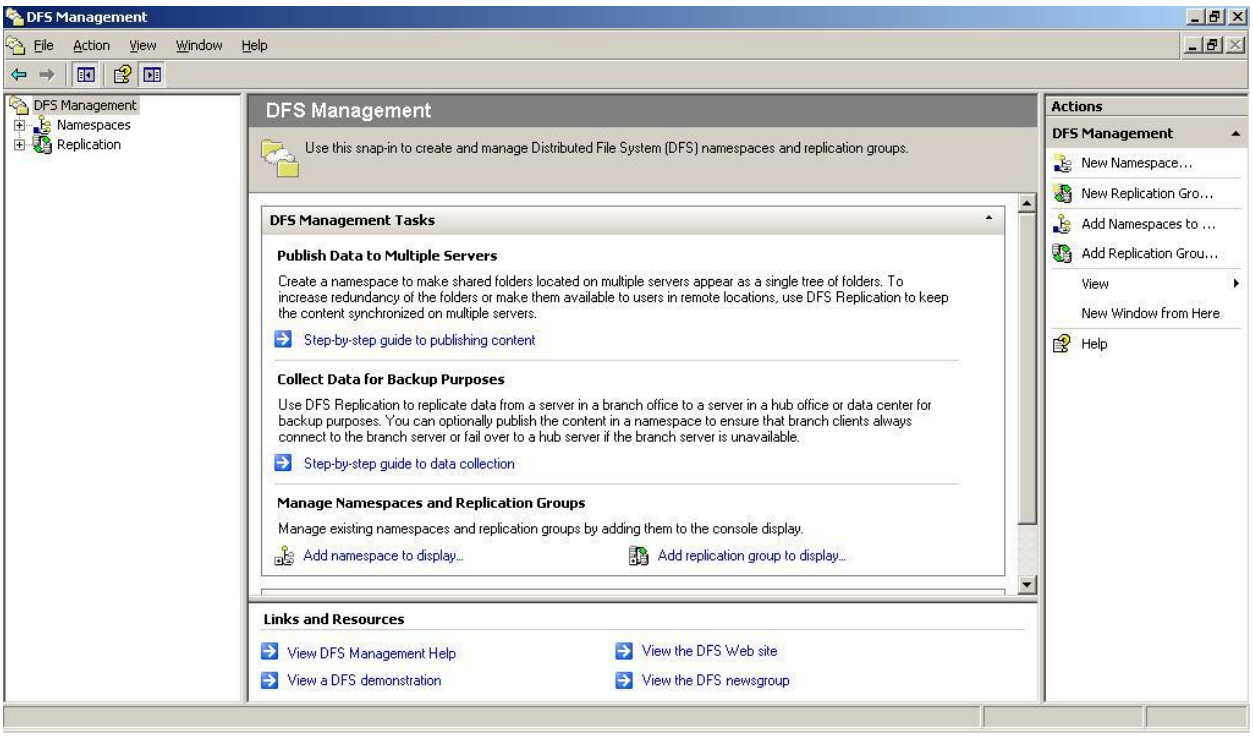


Copyright © 2008 Microsoft Corporation.

All rights reserved.

Distributed File System (DFS) Management Snap-in

Administrators can use the Distributed File System (DFS) Management snap-in to configure and manage DFS Namespaces and DFS Replication. When used together, these two technologies offer simplified, fault-tolerant access to files, load sharing, and WAN-friendly replication. The snap-in provides integration between the two Distributed File System components so that administrators can select an existing folder in a namespace and configure DFS Replication on the folder targets (shared folders) associated with the folder, and also add a replicated folder to an existing namespace.



Active Directory Federated Services (ADFS) interfaces

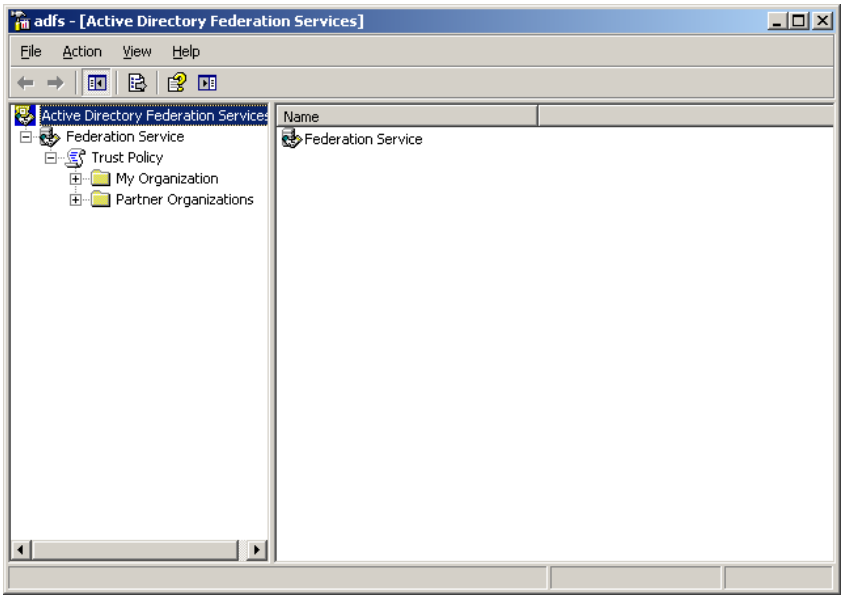
This subsection provides a brief description of the management interfaces used to configure Active Directory Federation Services (ADFS).

ADFS Management interface

The Active Directory Federation Services snap-in for the Microsoft Management Console (MMC) is used to configure ADFS trust policy, account stores, ADFS-enabled applications, and organization claims.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Trust Policy Properties interface

The **Trust Policy** node in the Active Directory Federation Services snap-in represents the trust policy configuration information that is stored in the trust policy file. The trust policy file is stored in .xml file format. It is created during setup of the federation server. The trust policy file path is configured in the local Web.config file.

> **Note:** It is strongly recommended that administrators use the Trust Policy node to edit trust policy configuration information. Do not edit the policy information in the file manually.

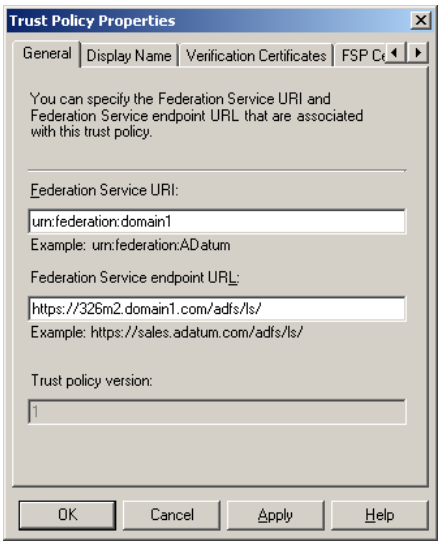
The **Trust Policy** node in the management console manages claims and federation trust relationships. **Trust Policy** contains two main elements:

- **My Organization:** For configuring items that deal directly with the local organization. This includes organization claims, account stores, and applications.
- **Partner Organizations:** For configuring trust relationships with other organizations. This includes account partners and resource partners.

The Trust Policy properties pages are used to configure the organization (or realm's) Display Name, the Verification Certificates required to establish a trust, the Federation Server Proxy (FSP) certificate required if the Federation Service Proxy is running on another computer that is acting as a proxy to the local federation server, Event Log levels, Transform Modules (where applicable), and other Advanced properties (such as token caching timeout periods).

Copyright © 2008 Microsoft Corporation.

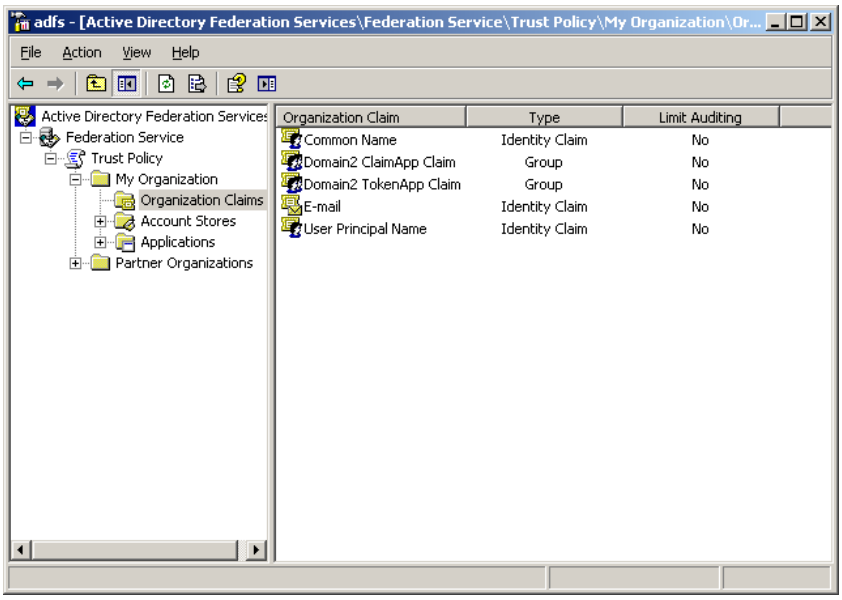
All rights reserved.



My Organization interfaces

The **My Organization** node in the console tree of the Active Directory Federation Services snap-in provides an interface used to configure trust policy settings in the Federation Service for which the local organization has administrative control, including:

- **Organization:** For defining a set of claims that the local organization understands.
- **Account Stores:** For mapping attributes and identities to organization claims.
- **Applications:** For enabling and disabling the passing of claims to either claims-aware applications or Windows NT token-based applications.



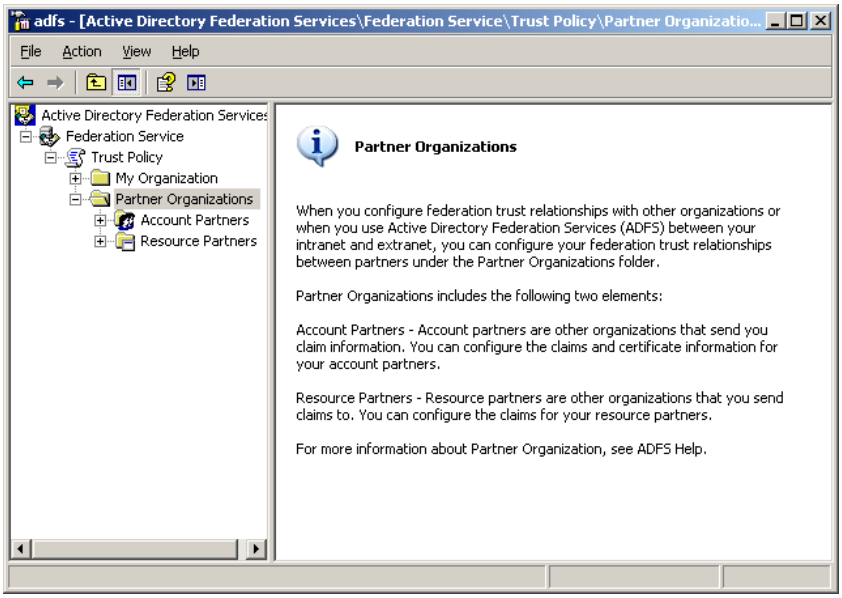
Copyright © 2008 Microsoft Corporation.

All rights reserved.

Partner Organizations interfaces

The **Partner Organizations** node in the Active Directory Federation Services snap-in is used in federated Web SSO scenarios for configuring federation trust relationships between partners and includes the following two elements:

- **Account Partners:** For configuring other organizations that send claims information to the local organization. Use this interface to configure claims and certificate information for account partners.
- **Resource Partners:** For configuring other organizations to which the local organization sends claims. Use this interface to configure claims for resource partners.

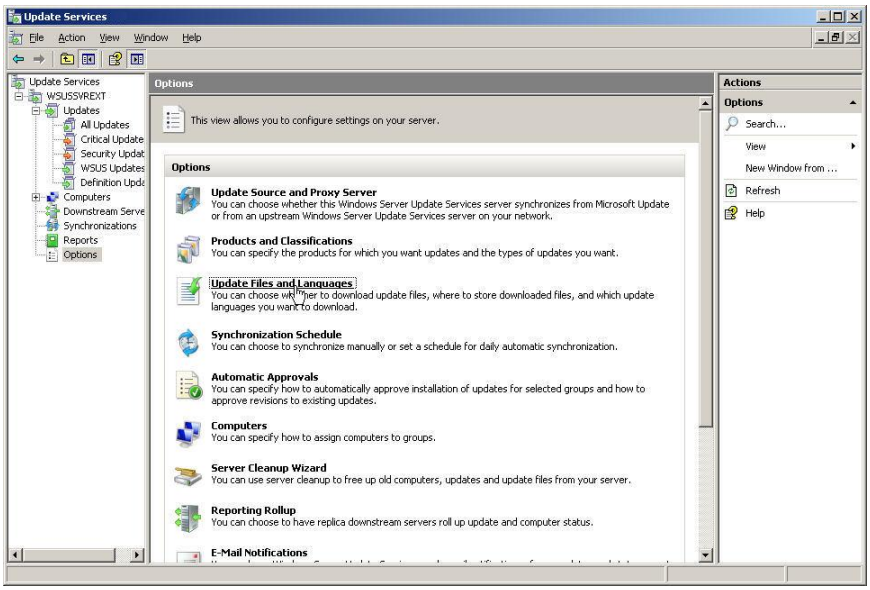


Windows Server Update Services (WSUS) interface

The Update Services interface allows WSUS administrators to specify the types of updates to download, create target groups of computers to receive updates, and determine which computers require updates before deployment. WSUS administrators can also approve updates for automatic deployment, uninstall updates, and generate reports to monitor update activity.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

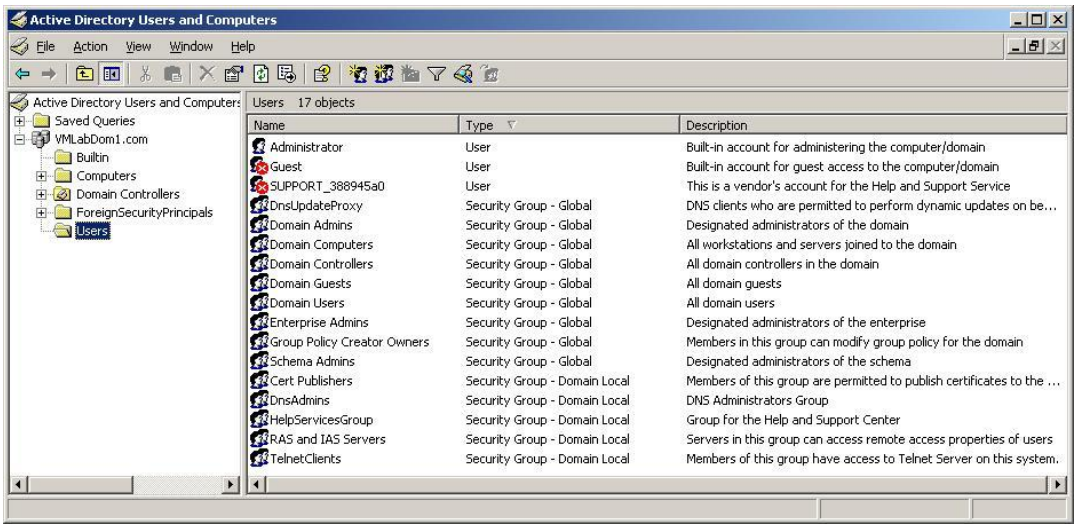


Account Management Tools

Windows Server 2003 provides specific tools for managing user, group, and computer accounts depending whether accounts are local to a computer or are defined at the domain level.

Active Directory Users and Computers

The **Active Directory Users and Computers** interface is used to create and manage users, groups, computers, and other Active Directory objects for a domain and is only available on Domain Controllers.



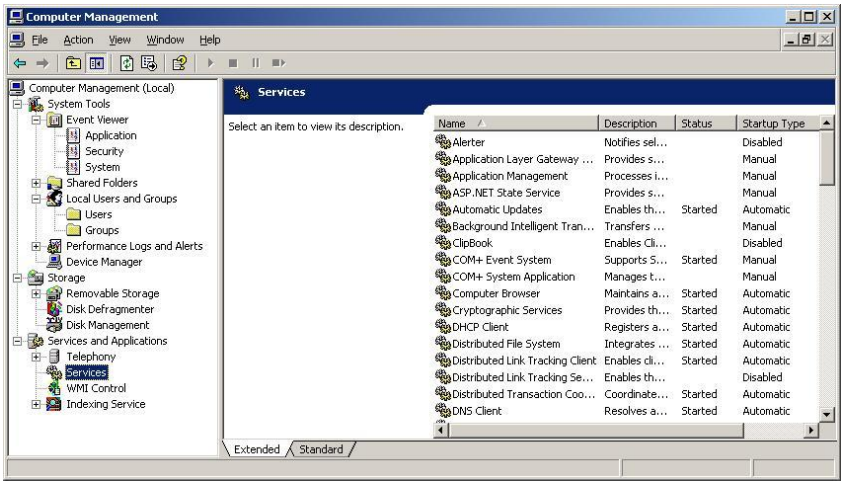
Computer Management

The **Computer Management** interface is available on all Windows Server 2003 operating systems. It supports management of audit logs, share assignments and permissions, system services, as well as

Copyright © 2008 Microsoft Corporation.

All rights reserved.

user and group accounts. On Domain Controllers, the user and group accounts are managed from the **Active Directory Users and Computers** interface instead of the **Computer Management** interface.

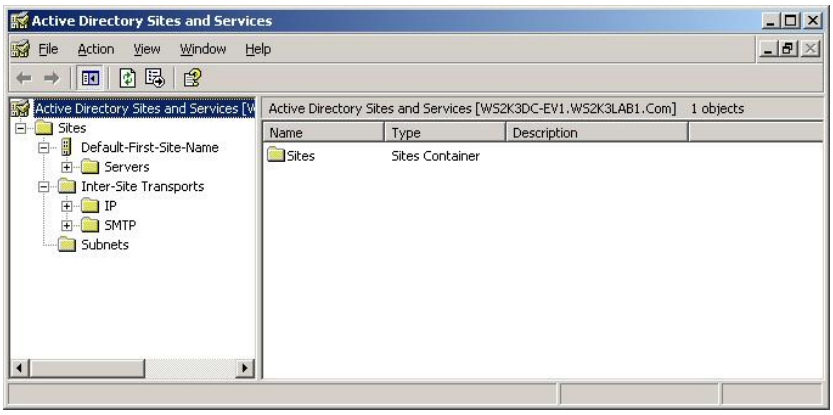


Active Directory Management

Active Directory management functions addressed in this document include data replication and administration of trust relationships.

Active Directory Sites and Services

The **Active Directory Sites and Services** tool is used to administer the replication of directory data. Active Directory Sites and Services can only be used from a computer that has access to a Windows Server 2003 domain. **Active Directory Sites and Services** is installed on all Windows Server 2003 Domain Controllers.

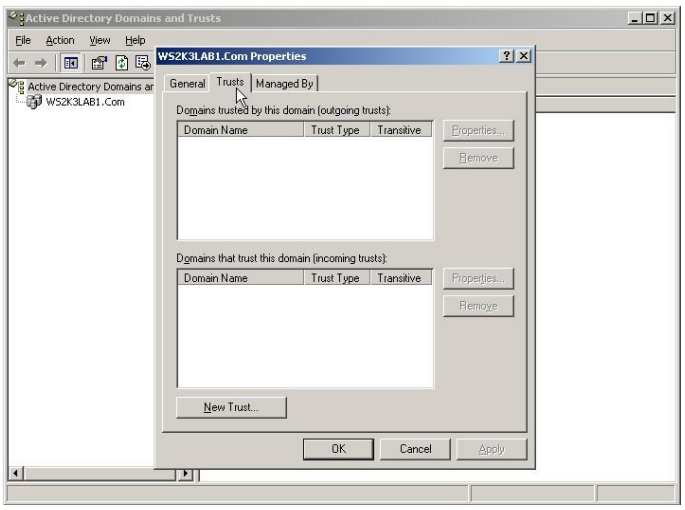


Active Directory Domains and Trust

The **Active Directory Domains and Trusts** tool is used to administer domain trusts, add user principal name suffixes, and change the domain mode.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



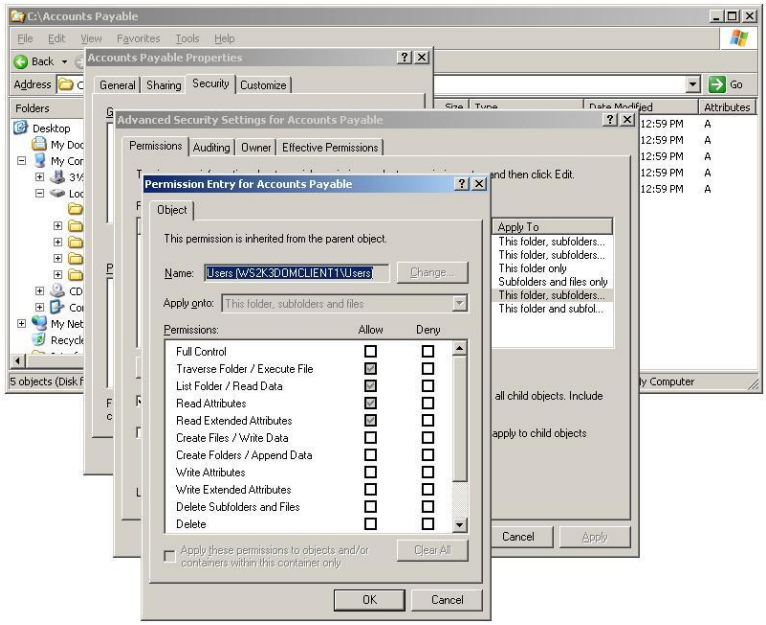
System Security Configuration, Maintenance, and Monitoring

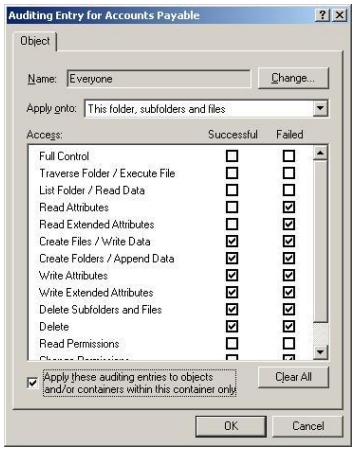
A variety of tools are available for configuring and enforcing security on Windows Server 2003 operating systems. Specific tools addressed within this document are identified in this section.

Windows Explorer

The **Windows Explorer** interface is used to navigate the folders and directories on the local hard drives, share connections, and network resources. Security management features associated with Windows Explorer include:

- Setting NTFS permissions;
- Setting audit requirements on objects; and
- Setting EFS properties on objects.



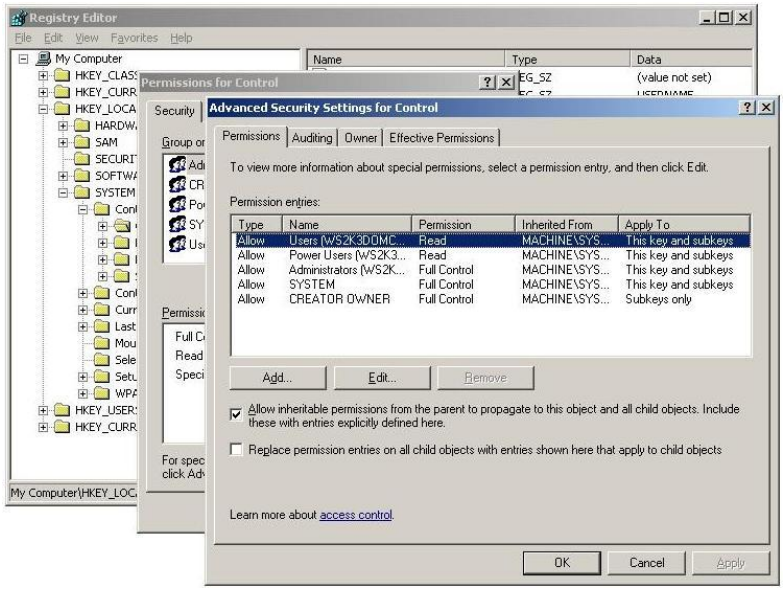


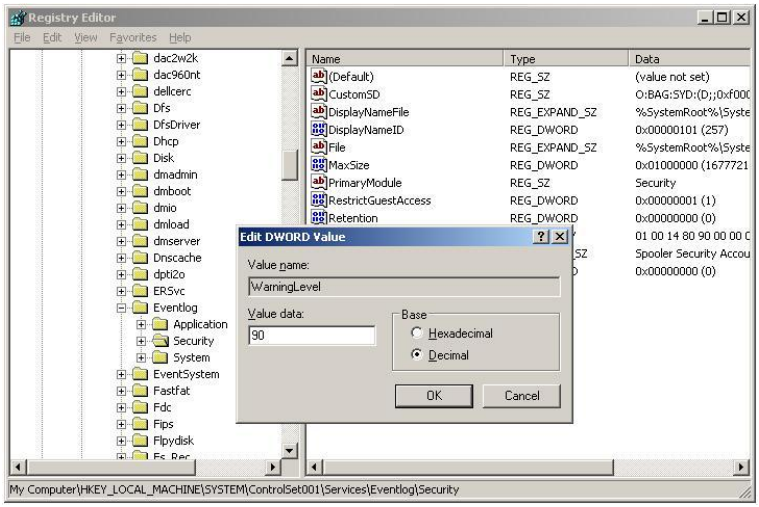
Copyright © 2008 Microsoft Corporation.
All rights reserved.

Registry Editor

Windows Server 2003 includes a **Registry Editor** (regedit.exe) that can be used to set specific values within the system Registry. Security management features associated with the Registry Editor include:

- Setting Registry permissions on Registry keys;
- Setting audit requirements on Registry keys; and
- Applying and modifying security configuration settings for system behavior.





> **Warning:** Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

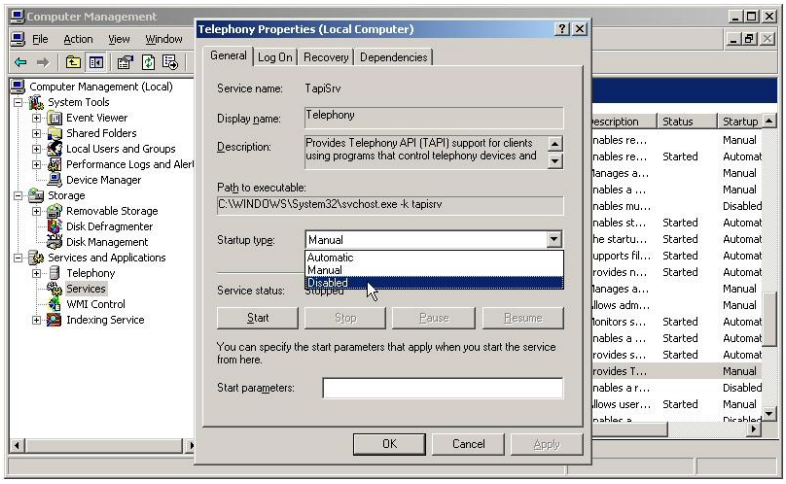
System Services

The **Services** tool is used to manage the services on a Windows Server 2003 computer, set recovery actions to take place if a service fails, and create custom names and descriptions for services. **Services**

Copyright © 2008 Microsoft Corporation.

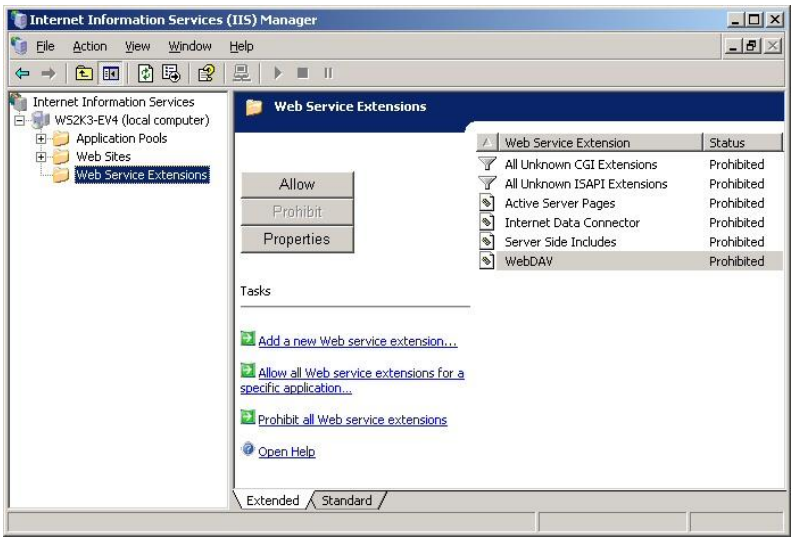
All rights reserved.

can be accessed from the **Computer Management** interface, or can be accessed as an individual tool object from the **Administrative Tools** menu.



IIS Manager

IIS Manager is a graphical interface for configuring application pools or Web, File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), or Network News Transfer Protocol (NNTP)[5] sites. IIS Manager can be used to configure IIS security, performance, and reliability features. It is used to add or delete sites; start, stop, and pause sites; back up and restore server configurations; and create virtual directories for content management.

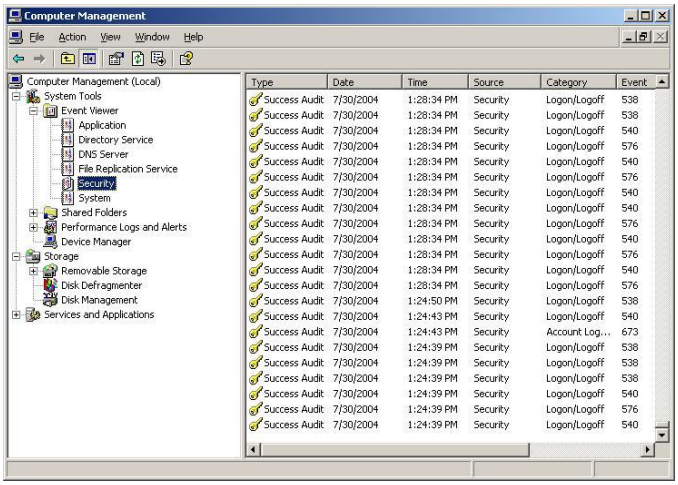


[5] FTP, SMTP, and NNTP are not part of the TOE.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

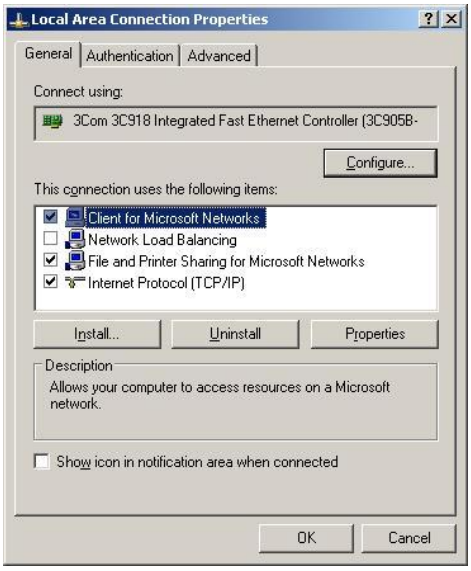
Event Viewer

Event Viewer is used to view and manage logs of system, program, and security events on a Windows Server 2003 computer. **Event Viewer** gathers and logs information about hardware and software problems, and monitors Windows Server 2003 security events. Authorized administrators can use Event Viewer's filtering and search capabilities to tailor their view of the event logs and locate specific events.



Local Area Connection

The **Local Area Connection Properties** interface is used in configuring the computer for network communications. It is used to set network addressing information on the computer and specify the protocols and network services that it will support.

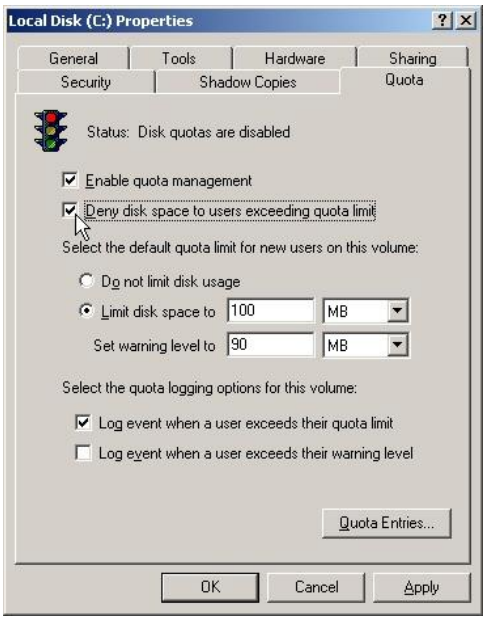


Disk Quota

The disk quota management interface allows an authorized administrator to manage disk quotas for NTFS volumes. More specifically, the functions allow an authorized administrator to enable or disable disk quotas, define default disk quotas, and define actions to take when disk quotas are exceeded.

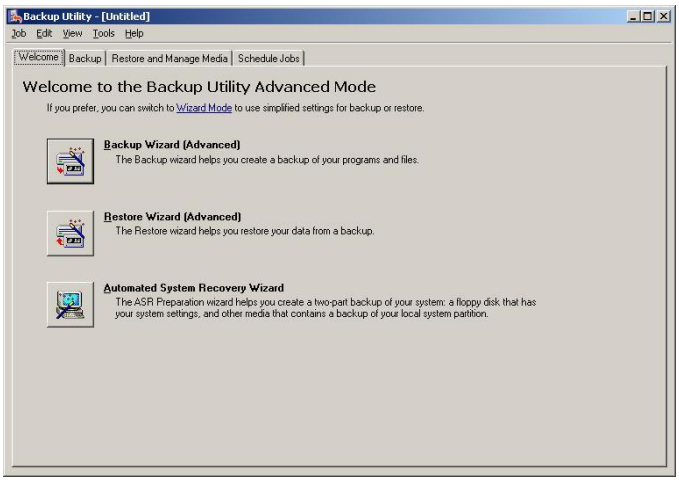
Copyright © 2008 Microsoft Corporation.

All rights reserved.



Backup

The **Backup** utility is used to backup important user information and system configuration files for backup protection. **Backup** can create a duplicate copy of all of the data on a hard disk and then archive it on another storage device.



Error Checking Tool

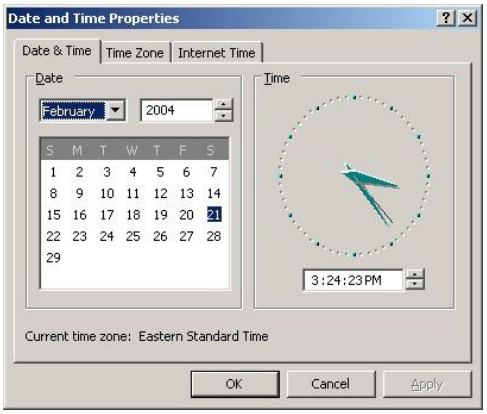
The error-checking tool is used to ensure the integrity of the file system by checking for file system errors and bad sectors on the hard disk.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

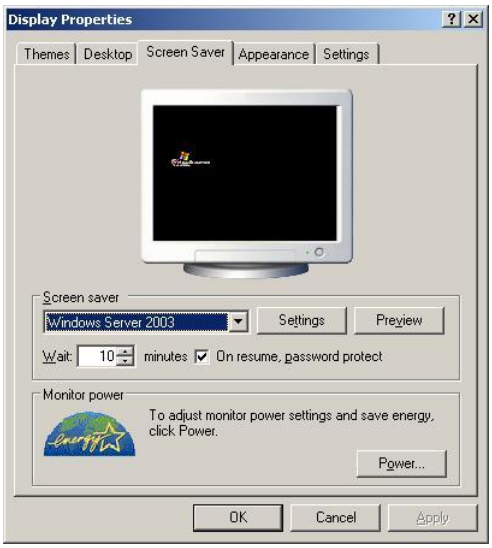
Date/Time Properties

Computer time settings are set during the setup process, but can be changed by the administrator at any time through the **Date/Time Properties** GUI.



Display Properties

The **Display Properties** interface is used to protect a computer from unauthorized access by setting a password-protected screensaver that will automatically initiate after a set period of inactivity.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

Configuration Wizards

A number of configuration wizards are available in Windows Server 2003. The configuration wizards provide a simplified step-by-step method for using or setting security features in Windows Server 2003. Examples of available configuration wizards are described below.

Active Directory Installation Wizard

The **Active Directory Installation Wizard** is used in converting a Windows Server 2003 computer into a Domain Controller by installing Active Directory services.

Delegation of Control Wizard

The **Delegation of Control Wizard** allows an authorized administrator to delegate administration of a domain or Organizational Unit (OU).

Security Configuration Wizard

The **Security Configuration Wizard** (SCW) is a new tool that is available with the installation of Windows Server 2003 Service Pack 1 (SP1) and higher. The SCW reduces the attack surface of Microsoft Windows 2003 Servers by guiding an authorized administrator through a series of questions designed to determine the functional requirements of a server. Any service functionality that is not required, by the roles being performed by the server, is then disabled. This provides greater security for the server by eliminating the potential of those services being used as an avenue of attack.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

IP Security Policy Wizard

The **IP Security Policy Wizard** can be used to tailor an IPSec policy to suit the particular security needs and requirements of an organization.

Security Rule Wizard

The **Security Rule Wizard** guides an administrator in defining the security actions that must be activated when network communications meet a specified set of criteria.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Certificate Export and Import Wizards

The **Certificate Export** and **Import Wizards** assist the administrator in backing up and restoring user certificates.

Security Functions

This subsection identifies all the security functions available to the administrator and needed to operate Windows Server 2003 securely. The details regarding security parameters and values are provided in the Graphical User Interface (GUI) specifications. The administrative security functions are derived from the Windows Server 2003 security functions described in the Windows 2003/XP V3 ST.

The TOE supports a number of policies and features that require appropriate management. With few exceptions, the security management functions are restricted to an authorized administrator. This constraint is generally accomplished by privilege or access control (i.e., security descriptor), and occasionally by a specific Security Identifier (SID) requirement (i.e., "Administrators"). Windows Server 2003 supports security management functions for the following security policies and features:

Account Policy – The account policy management functions allow only an authorized administrator to define constraints for passwords (password complexity requirements), account lockout (due to failed logon attempts) parameters, and Kerberos key usage parameters. The constraints for passwords restrict changes by including minimum password length, password history, and the minimum and maximum allowable password age. If the maximum password age is exceeded, the corresponding user cannot logon until the password is changed. The account lockout parameters include the number of failed logon attempts (in a selected interval) before locking the account and setting the duration of the lockout. The Kerberos key usage parameters primarily specify how long various keys remain valid. While an authorized administrator can change passwords and a user can change their own passwords, Windows Server 2003 does not allow any user (including the authorized administrator) to read passwords.

Account Database – The account database management functions allow an authorized administrator to define, assign, and remove security attributes to and from both user and group accounts, both locally and

Copyright © 2008 Microsoft Corporation.

All rights reserved.

for a domain, if applicable. The set of attributes includes account names, SIDs, passwords, group memberships, and other security-relevant and non-security relevant information. Of the set of user information, only the password can be modified by a user that is not an authorized administrator. Specifically, an authorized administrator assigns an initial password when an account is created and may also change the password like any other account attribute. However, users have the ability to change their own password. This capability is controlled by requiring users to first enter their old password in order to change the password to a new value.

Audit Policy – The audit policy management functions allow an authorized administrator the ability to enable and disable auditing, to configure which categories of events will be audited for success and/or failure, and to manage (create, delete, and clear) and access the security event log. An authorized administrator can also define specifically which user and access mode combinations will be audited for specific objects in the system.

Cryptographic Policy – A Cryptographic Policy can be set to determine if the Transport Layer Security (TLS)/Secure Sockets Layer (SSL) Security Provider supports only the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite. In effect, this means that the provider only supports the TLS protocol as a client and as a server (if applicable). It uses only the Triple Data Encryption Standard (DES) encryption algorithm for the TLS traffic encryption, only the Rivest, Shamir, and Adleman (RSA) public key algorithm for the TLS key exchange and authentication, and only the Secure Hashing Algorithm 1 (SHA-1) for the TLS hashing requirements.

Domain Policy – The domain management functions allow an authorized administrator to add and remove machines to and from a domain as well as to establish trust relationships among domains. Changes to domains and domain relationships effectively change the definition and scope of other security databases and policies (e.g., the account database). For example, accounts in a domain are generally recognized by all members of the domain. Similarly, accounts in a trusted domain are recognized in the trusting domain.

Firewall Policy – The group policy management functions allow an authorized administrator to define a Windows Firewall policy for a group of Windows Server 2003 and Windows XP Professional computers within a domain.

Group Policy – The group policy management functions allow an authorized administrator to define accounts, user right assignments, and machine/computer security settings, etc. for a group of Windows Server 2003 systems or accounts within a domain. The group policies effectively modify the policies (e.g., machine security settings, and user rights policy) defined for the corresponding systems or users.

IPSec Policy – The IPSec management functions allow an authorized administrator to define whether and how (e.g., protocols and ports to be protected, outbound and/or inbound traffic, with what cryptographic algorithms) IPSec will be used to protect traffic among distributed Windows Server 2003 systems.

EFS Policy – The EFS management functions allow an authorized administrator to enable or disable EFS on NTFS volumes and generally control the recovery for EFS data.

File Encryption Key (FEK) Policy - Only the owner of the private key used to protect the FEK associated with the file or an administrator or subject with a specific privilege can delete the FEK.

Disk Quota Policy – The disk quota management functions allow an authorized administrator to manage disk quotas for NTFS volumes. More specifically, the functions allow an authorized administrator to enable or disable disk quotas, define default disk quotas, and define actions to take when disk quotas are exceeded.

Discretionary Access Control (DAC) Policy – The DAC functions allow authorized users to modify access control attributes associated with a named object.

Public Key Infrastructure (PKI) Policy – Windows Server 2003 clients support PKI policies for certificate auto-enrollment.

Smart Card Usage Policy – Policies can be set to require the use of smart cards and to modify the behavior of the computer when a smart card is removed.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

System Banner – The logon functions can be configured by authorized administrators to display an advisory warning message before access to the TOE is granted.

Session Locking – Windows Server 2003 provides the ability for users to lock their sessions immediately or after a defined interval. It constantly monitors the mouse and keyboard for activity and locks the workstation after a set period of inactivity. Unlocking any locked session is restricted to administrators and the interactively logged on user.

Time – Setting the system clock is restricted to administrators.

User Rights Policy – The user rights management functions allow an authorized administrator to assign or remove user and group accounts to and from specific logon rights and privileges.

Windows Server 2003 Security Policies

Windows Server 2003 allows authorized administrators the ability to establish security settings in a Local Group Policy Object (LGPO) for any computer, regardless of whether it participates in an Active Directory domain or not. For all computers participating in domain, the LGPO is processed first, followed by any site, domain, or OU policies. If a computer is participating in a domain and a conflict occurs between domain and local computer policy, the domain policy prevails. However, if a computer is no longer participating in a domain, the LGPO is applied.

Group Policies are administered through the use of Group Policy Objects (GPOs), data structures that are attached in a specific hierarchy to selected Active Directory Objects, such as Sites, Domains, or OUs. These GPO's, once created, are applied in a standard order: Local, Site, Domain, OU, with the later policies being superior to the earlier applied policies.

Account policies (password, lockout, Kerberos) are defined for the entire domain in the default domain GPO. Local policies (audit, user rights, and security options) for Domain Controllers are defined in the default Domain Controllers GPO. For Domain Controllers, settings defined in the default Domain Controller GPO have higher precedence than settings defined in the default Domain GPO. Thus, if a user privilege (for example, Add workstations to domain) were to be configured in the default Domain GPO, it would have no impact on the Domain Controllers in that domain.

> **Note:** The Account Policies security area receives special treatment in how it takes effect on computers in the domain. All Domain Controllers in the domain receive their account policies from GPOs configured at the domain node regardless of where the computer object for the Domain Controller is. This ensures that consistent account policies are enforced for all domain accounts. All non-Domain Controller computers in the domain follow the normal GPO hierarchy for getting policies for the local accounts on those computers. By default, member workstations and servers enforce the policy settings configured in the domain GPO for their local accounts, but if there is another GPO at lower scope that overrides the default settings, then those settings will take effect.

Subsections Local Security Policy, Domain Security Policy, and Domain Controller Security Policy provide the procedures for accessing the security policy interfaces for the Local Security Policy, the Domain Security Policy, and the Domain Controller Security Policy. Subsections Account Policies and Local Policies describe how the interfaces are used to set and manage security policies. A list of security policy default settings and Evaluated Configuration required changes are available in Appendices A and E, respectively, of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Local Security Policy

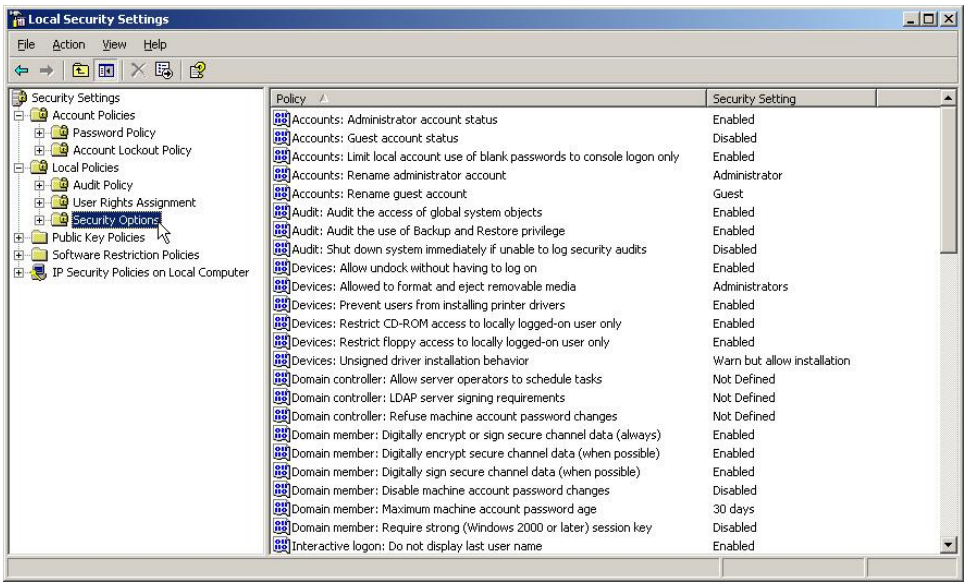
Since stand-alone computers are not part of Active Directory, group policies do not apply to them. To view and edit a local security policy:

1. Log on to the as an authorized administrator.

Copyright © 2008 Microsoft Corporation.

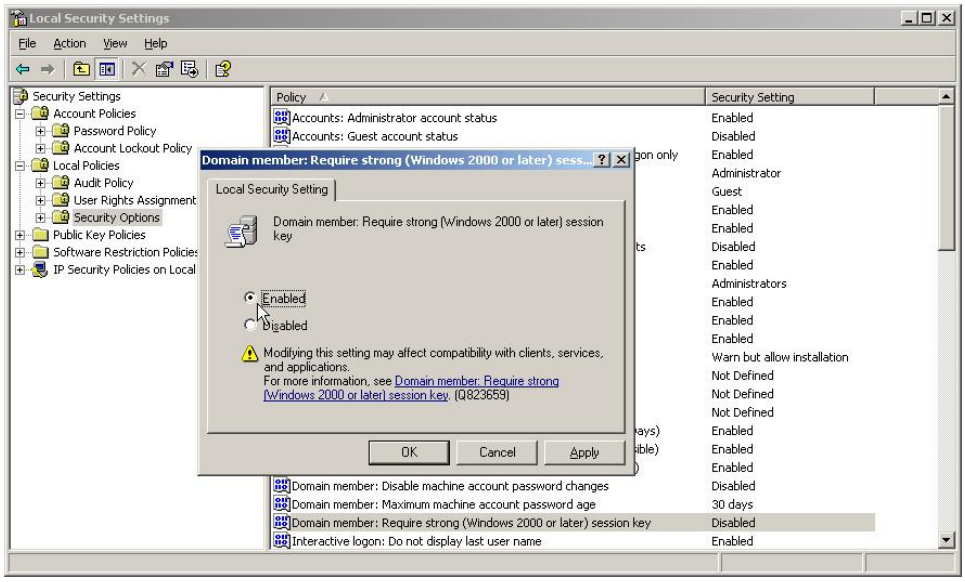
All rights reserved.

2. Click **Start**, point to **Administrative Tools**, and then click **Local Security Policy**. This opens the **Local Security Settings** interface.



3. Open the items in the tree to find the policy that is to be changed.

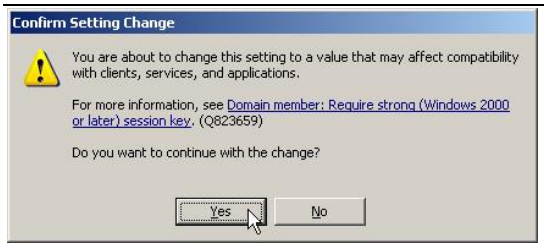
4. Double-click the policy, make the change, and then click **OK**.



Note: Some setting changes may have an impact on the compatibility between clients, services, and applications. Attempting to make changes to these settings will result in a confirmation notice such as the one shown below:

Copyright © 2008 Microsoft Corporation.

All rights reserved.



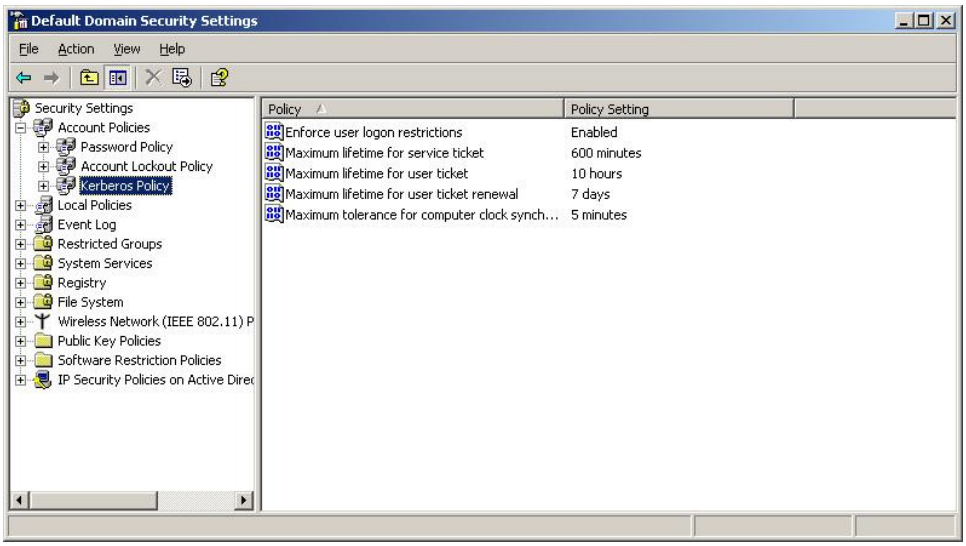
Review the information provided by the notice and proceed as necessary.

5. Close the Local Security Settings interface.

Domain Security Policy

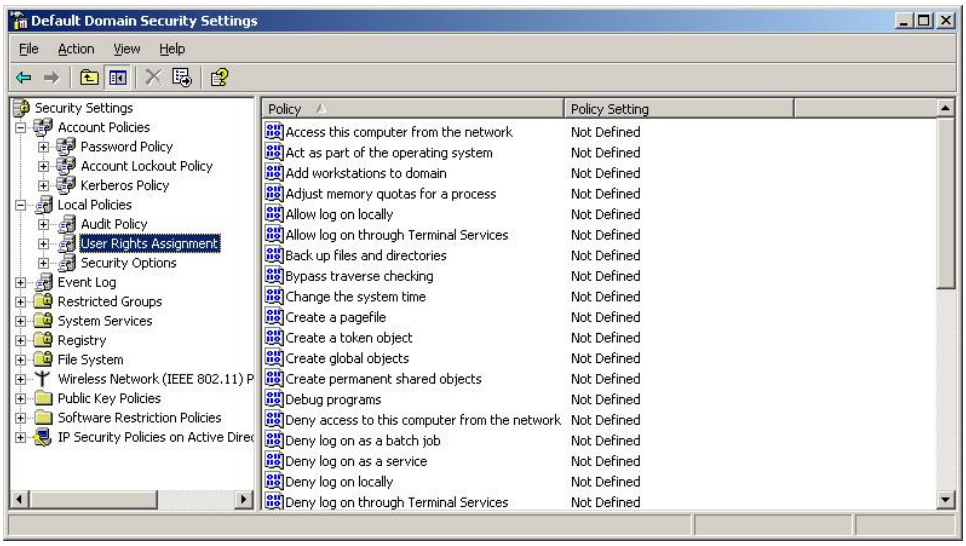
To view and edit a domain-wide security policy:

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings interface**.
3. Expand **Account Policies** and then select **Password Policy**, **Account Policy**, and **Kerberos Policy** in sequence to view their settings. In the results pane, notice that the settings within **Password Policy**, **Account Lockout Policy**, and **Kerberos Policy** are configured by default in the domain GPO, and thus apply to all computers within that domain.



4. Next, navigate to **Local Policies**.
5. Click the **User Rights Assignment** subfolder. Notice that, by default, none of the user rights are defined in the **Domain Security Policy**. This does not mean that user rights are not defined for machines in throughout the enterprise, just that these rights are not defined by default in the **Domain Security Policy**. Once defined in the **Domain Security Policy**, the setting will override local and Site security policies. For Domain Controllers, the user rights are defined in the **Domain Controller Security Policy**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



6. Close the **Default Domain Security Settings** interface.

Note: Another method of viewing and modifying the Domain Security Policy is to access the Domain GPO.

Domain Controller Security Policy

The previous subsection, reviewed the domain policy configured by default for all new domains. This subsection, reviews the **Default Domain Controller Security Policy**, which specifies security settings for all machines in the Domain Controller OU. By default, all Windows Server 2003 Domain Controller computers within a domain are added to the same Domain Controller OU.

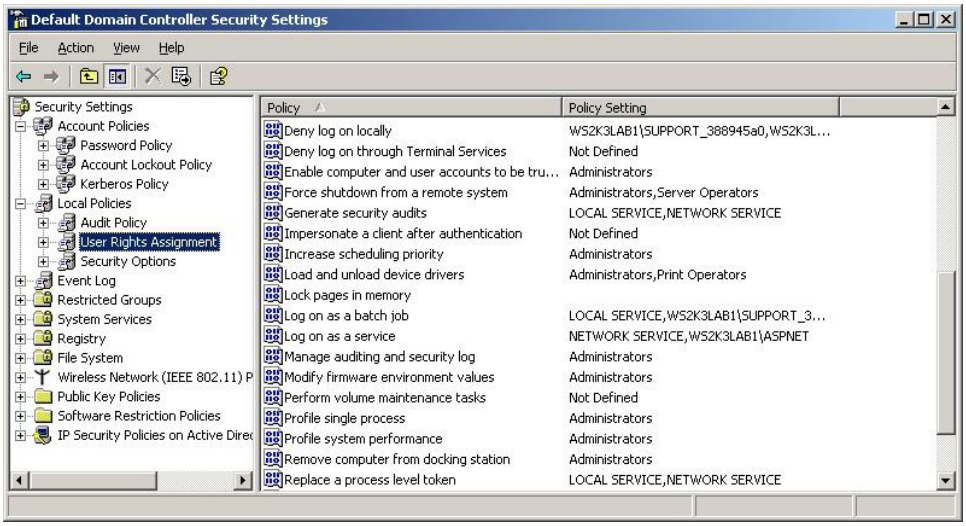
To view and edit a **Domain Controller Security Policy**;

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Controller Security Policy**. This opens the **Default Domain Controller Security Settings** interface.
3. Navigate to **Account Policies** and select **Password Policy**. In the results pane, notice that a **Password Policy** is not defined in the **Default Domain Controller Security Policy**, because Password Policy are defined for the entire **Domain Security Policy**. Since the **Account Policy** settings in the **Domain Security Policy** take precedence across the domain, any setting changes to Account Policy settings within the **Domain Controller Security Policy** will have no effect.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

4. Navigate to **Local Policies**, and select **User Rights Assignments**. In the results pane, note that user rights are configured in the default Domain Controller OU. Since the **Domain Controller Security Policy** is defined as an OU policy, all **Local Policy** settings, with the exception of several "account" **Security Options**, within the **Domain Controller Security Policy** will override any such settings define in the **Domain Security Policy**. The same holds true for other policy setting within the OU, such as **Event Log**, **Restricted Groups**, **System Services**, etc.



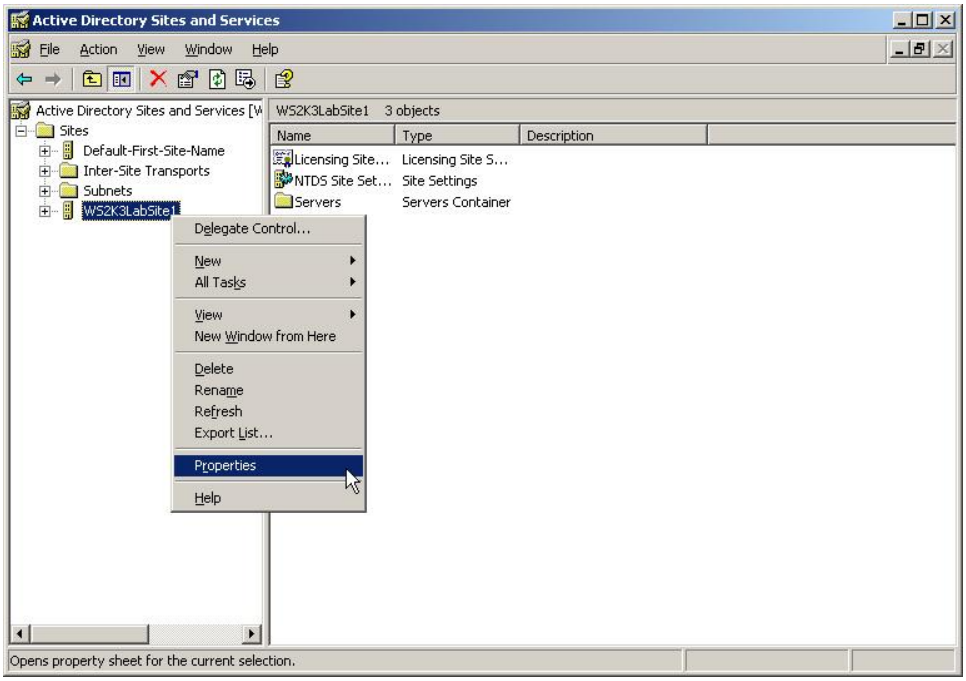
Site GPO's

To view and edit a Site GPO;

1. Log on to the Domain Controller as authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**. Expand the **Sites** folder, right click on the desired site and select **Properties**.

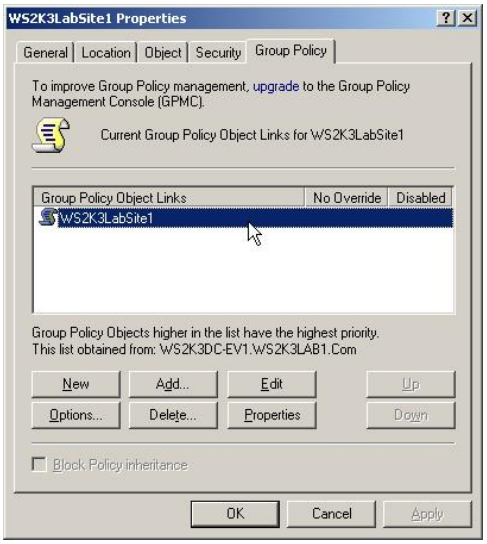
Copyright © 2008 Microsoft Corporation.

All rights reserved.



Note: The name of the first site **Default-First-Site-Name** may be changed. The first site contains the Domain Controller, but has no site policy set by default.

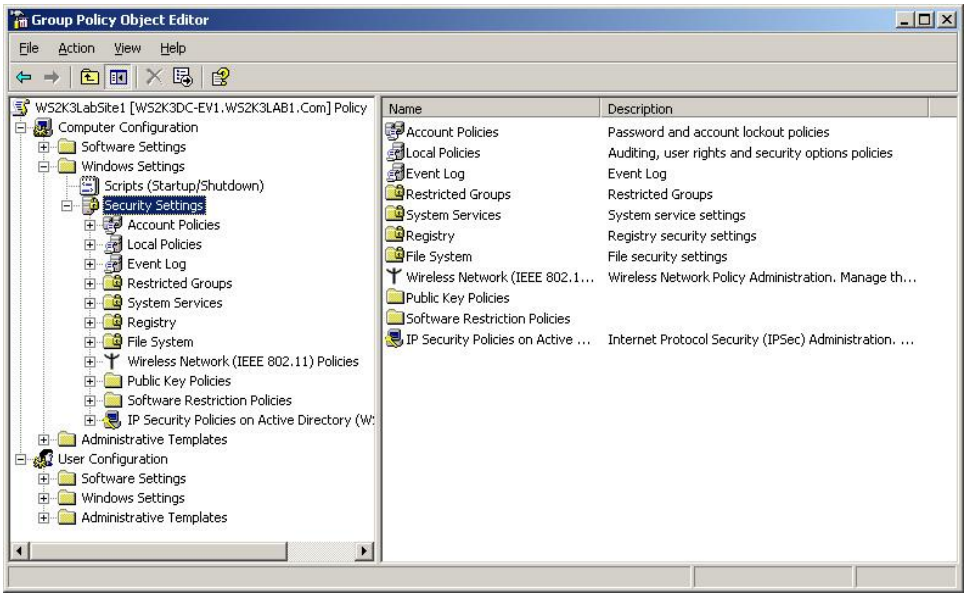
3. In the site **Properties** interface, select the **Group Policy** tab. Select the desired group policy object link and click the **Edit** button. The **Group Policy Object Editor** will appear.



4. All site-specific policy settings are accessible from the **Group Policy Object Editor**. To access and edit the site security policy settings, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.

Copyright © 2008 Microsoft Corporation.

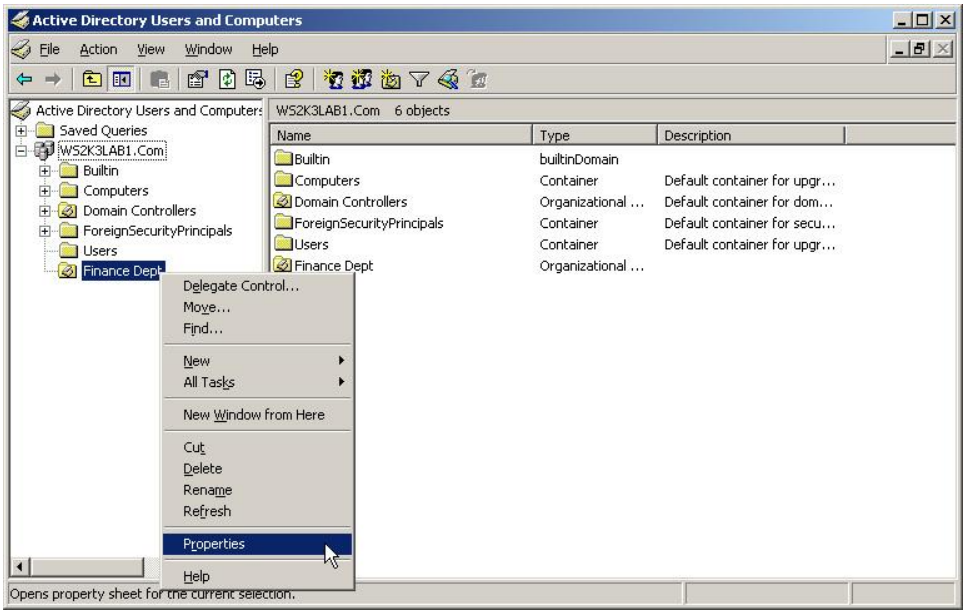
All rights reserved.



OU GPO's

To view and edit as OU GPO:

1. Log on to the Domain Controller as authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**. Expand the domain node, right click on the desired OU and select **Properties**.

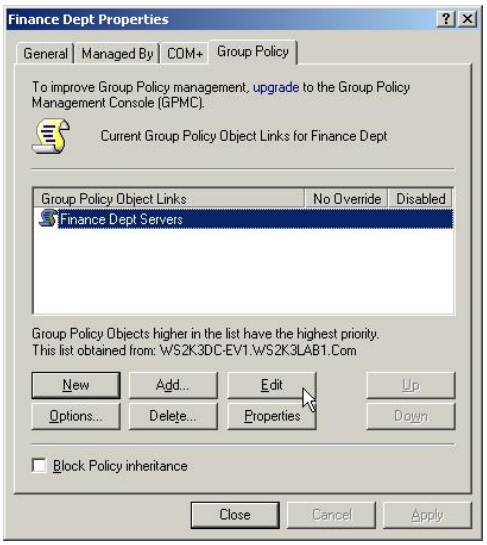


Note: A **Domain Controller's** OU exists by default. The **Domain Controller's** OU **Properties** interface provides an alternate means of accessing the Domain Controller security settings via the **Default Domain Controller's Policy** GPO. Likewise, the **Default Domain Policy** GPO may be accessed from the **Properties** interface of the domain object.

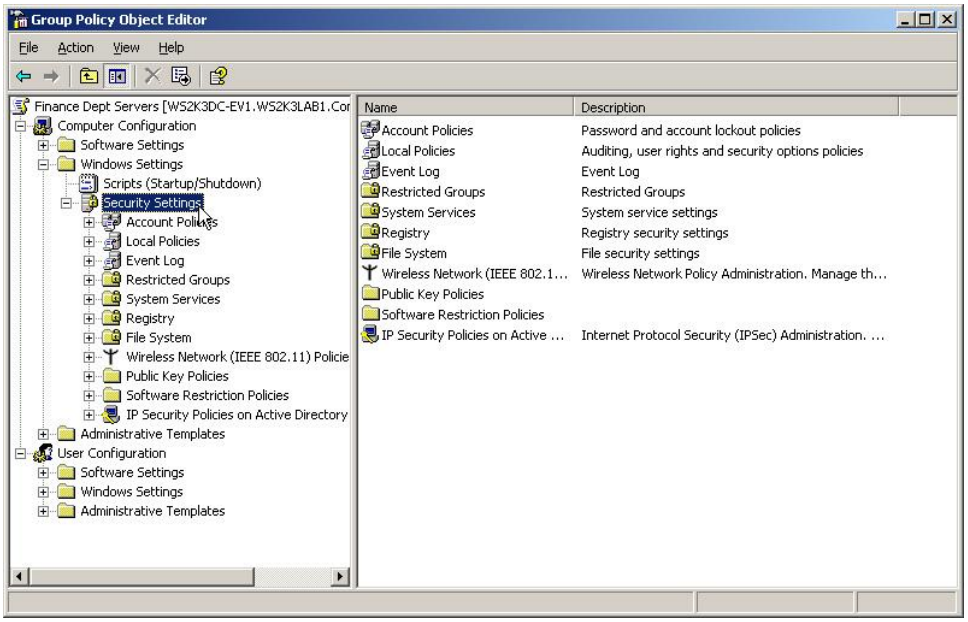
Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. In the OU **Properties** interface, select the **Group Policy** tab. Select the desired group policy object link and click the **Edit** button. The **Group Policy Object Editor** will appear.



4. All OU-specific policy settings are accessible from the **Group Policy Object Editor**. To access and edit the OU security policy settings, expand **Computer Configuration**, expand **Windows Settings**, and then expand **Security Settings**.



Account Policies

The policy settings under **Account Policies** are implemented at the domain level. A Windows Server 2003 domain must have a single password policy, account lockout policy, and Kerberos version 5 authentication protocol policy for the domain. Configuring these policy settings at any other level in Active Directory will only affect local accounts on member servers. If there are groups that require separate password policies, they should be segmented into another domain or forest based on any additional requirements.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

For domain accounts, there can be only one account policy per domain. The account policy must be defined in the **Domain Security Policy** or in a new policy that is linked to the root of the domain and given precedence over the **Default Domain Security Settings**, which is enforced by the Domain Controllers that make up the domain. A Domain Controller always pulls the account policy from a GPO linked to the domain, which by default is the **Default Domain Policy** GPO. This behavior occurs even if there is a different account policy applied to the OU that contains the Domain Controller.

By default, workstations and servers joined to a domain — the domain member computers — also receive the same account policy for their local accounts. However, local account policies for member computers can be differentiated from the domain account policy by defining an account policy for the OU that contains the member computers.

- **Password policy.** These policy settings are used for domain or local user accounts. They determine settings for passwords, such as enforcement and lifetimes.
- **Account lockout policy.** These policy settings are used for domain or local user accounts. They determine the circumstances and length of time that an account will be locked out of the system.
- **Kerberos Policy.** Kerberos authentication is the primary authentication mechanism used in an Active Directory domain. These policy settings are used for domain user accounts. They determine Kerberos-related settings, such as ticket lifetimes and enforcement.

Note: Kerberos Policy settings are only visible in the **Default Domain Security Settings** interface.

Configuring Password Policies

The security provided by a password system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known. In a password-based authentication mechanism implemented on a system, passwords are vulnerable to compromise at several essential stages related to password assignment, distributions, management, and use:

- A password must be initially assigned by an administrator and provided to a user when enrolled on the system;
- A user must change the initial password upon first logon;
- A user's password must be changed periodically;
- The system must maintain a "password database;"
- Users must remember their passwords;
- Users must enter their passwords into the system to authentication themselves; and
- Users may not disclose their passwords to anyone. This includes administrators and IT managers.

Note: Windows Server 2003 includes a Forgotten Password Wizard that may be used to create a Password Reset Disk. The Evaluated Configuration currently does not include the use of the Forgotten Password Wizard and the Password Reset Disk.

Password policies can be set depending on the needs of the organization. For example, it is possible to specify minimum password length, no blank passwords, and maximum and minimum password age. It is also possible to prevent users from reusing passwords and ensure that they use specific characters in their passwords, making the passwords more difficult to crack.

To access and configure **Password Policy** settings:

1. Log on as an authorized administrator.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: The examples that follow illustrate use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

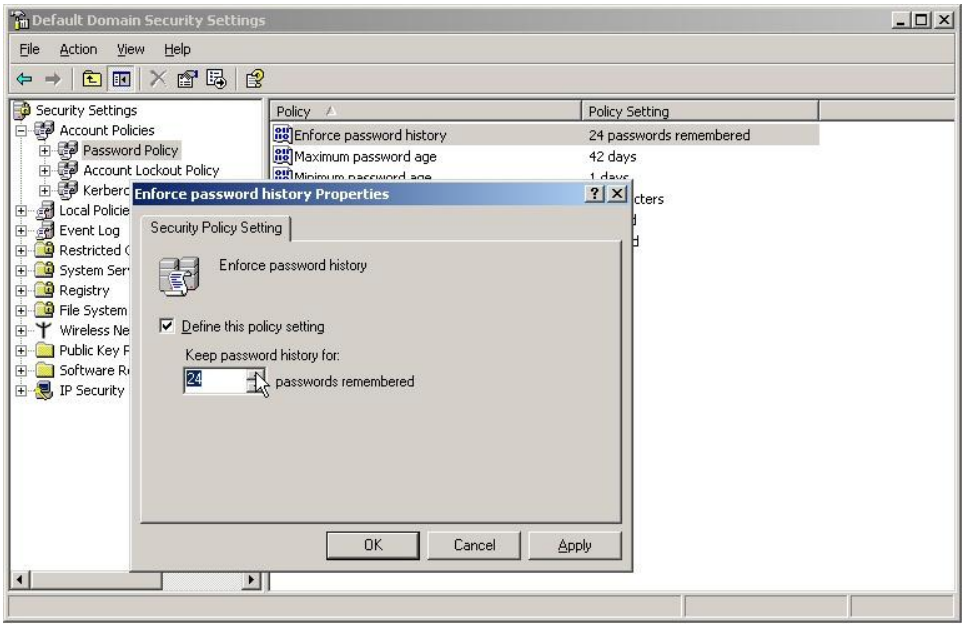
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Account Policies** and select **Password Policy**. The configurable password policy settings are presented in the right-hand details pane.
4. To edit a **Password Policy** setting, double-click on the policy setting or right-click it and select **Properties**.

The use of these policies are described and implemented as follows:

Note: Procedures for setting initial user passwords are provided in subsection Creating User Accounts of this document.

- **Enforce Password History:** The **Enforce password history** policy sets how frequently old passwords can be reused. This policy can be used to discourage users from changing back and forth between a set of common passwords. Windows Server 2003 can store up to 24 passwords for each user in the password history. By default, Windows Server 2003 has this setting at the maximum of 24 to best minimize vulnerabilities caused by password reuse.

  To disable this feature, set the size of the password history to zero (0). To enable this feature, set the size of the password history using the **passwords remembered** field. Windows Server 2003 will then track old passwords using a password history that is unique for each user, and users will not be allowed to reuse any of the stored passwords.



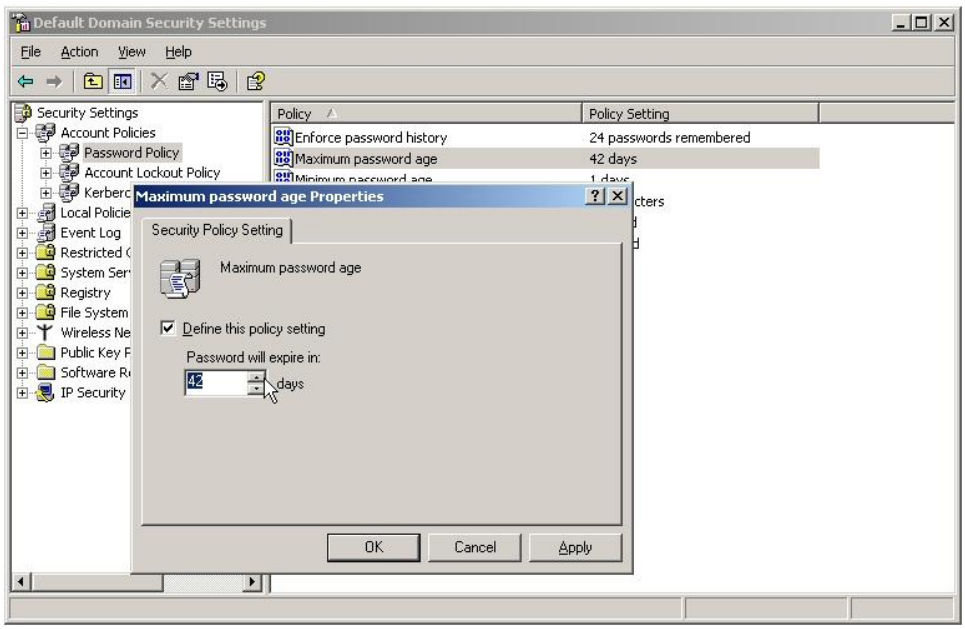
Note: To discourage users from cheating **Enforce password history**, they should not be allowed to change passwords immediately. This will prevent users from changing their passwords several times to get back to their old passwords. The **Minimum password age** setting can be used to prevent users from changing their passwords immediately.

- **Maximum Password Age:** The **Maximum password age** policy determines how long users can keep a password before they have to change it. The aim is to periodically force users to change their passwords. When this feature is used, set a value that makes sense for the specific network

Copyright © 2008 Microsoft Corporation.
All rights reserved.

environment it is being applied to. Generally, a shorter period is used when security is very important and a longer period when security is less important.

The default expiration date is 42 days; however, it can be set to any value from zero (0) to 999. A value of zero specifies that passwords do not expire. Although it may be tempting to set no expiration date, users should change passwords regularly to ensure the network's security. Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days.



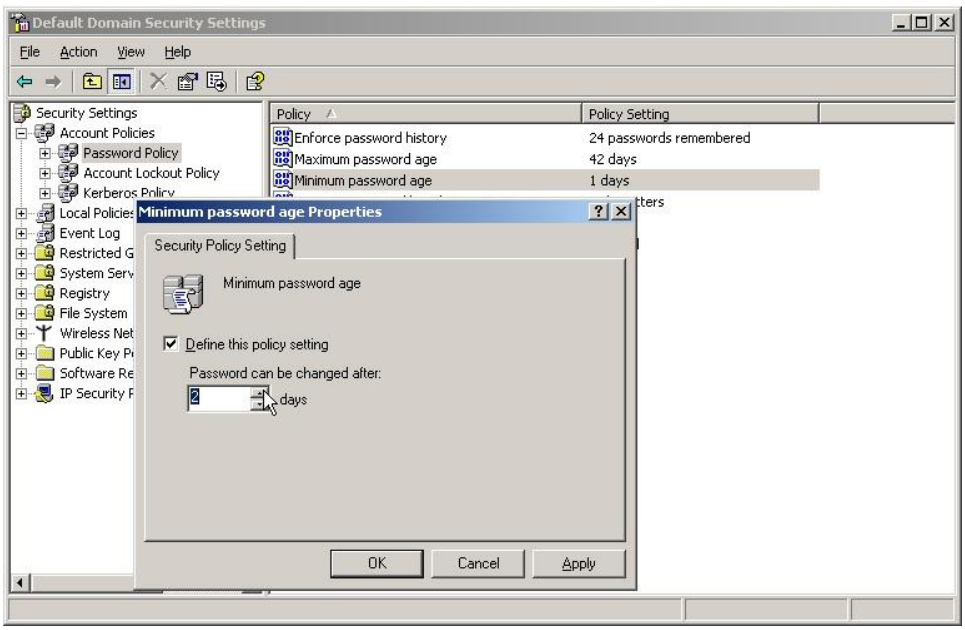
Note: For this policy to be effective, the Password never expires check box in the user account Properties interface must not be checked. Windows Server 2003 notifies users when they're getting close to the password expiration date. Anytime the expiration date is less than 30 days away, users see a warning when they log on stating that they have to change their password within so many days.

- **Minimum Password Age:** The **Minimum password age** policy determines how long users must keep a password before they can change it. This field can be set to prevent users from cheating the password system by entering a new password and then changing it right back to the old one.

  By default, the **Minimum password age** in Windows Server 2003 is set to zero on stand-alone servers and one (1) day on Domain Controller and in Domain Security Policies. For stronger security this setting can be increased. Reasonable settings are from two to seven days. In this way, users are less inclined to switch back to an old password but are able to change their passwords in a reasonable amount of time if they want to. A setting of zero (0) should never be used in the Evaluated Configuration since it would allow users to change their passwords immediately several times in order to bypass enforcement of the password history requirement.

Copyright © 2008 Microsoft Corporation.

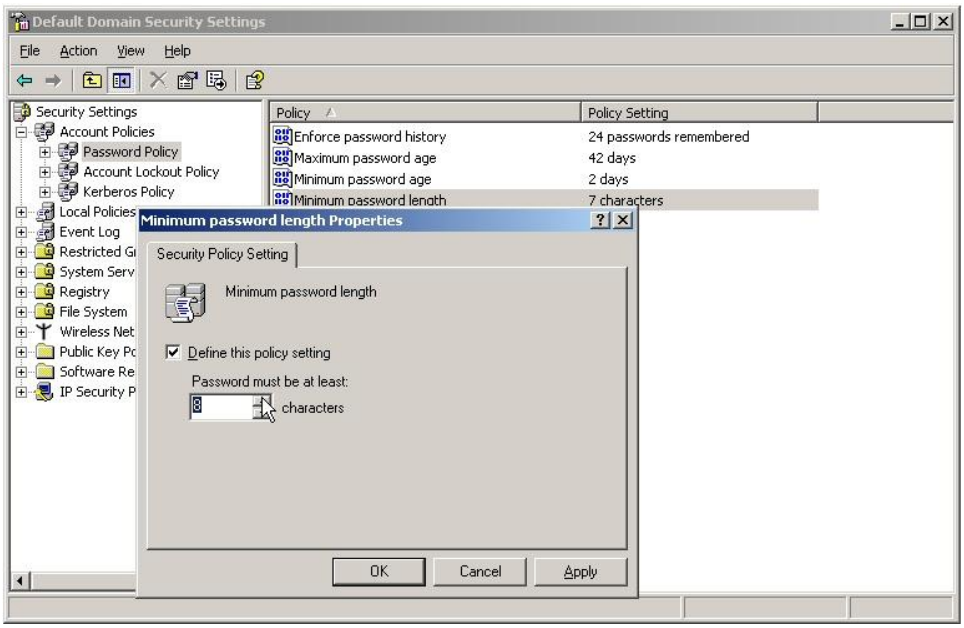
All rights reserved.



- **Minimum Password Length:** The **Minimum password length** policy sets the minimum number of characters for a password. If it hasn't been changed already, the default setting should be changed immediately. The default is to allow empty passwords (passwords with zero characters), which is definitely not a good idea.

  For security reasons, passwords of at least eight (8) characters are required. The reason for this is that long passwords are usually harder to crack than short ones. If greater security is needed, the minimum password length can be set to a maximum of 14 characters.

  Note: The minimum password length for the Evaluated Configuration is eight (8) characters.



- **Passwords Must Meet Complexity Requirements:** Beyond the basic password and account policies, Windows Server 2003 includes facilities for creating additional password controls. The functions implemented by enabling the **Passwords must meet complexity requirements** setting in **Password Policy** are enforced when a user or administrator attempts to change the password for a

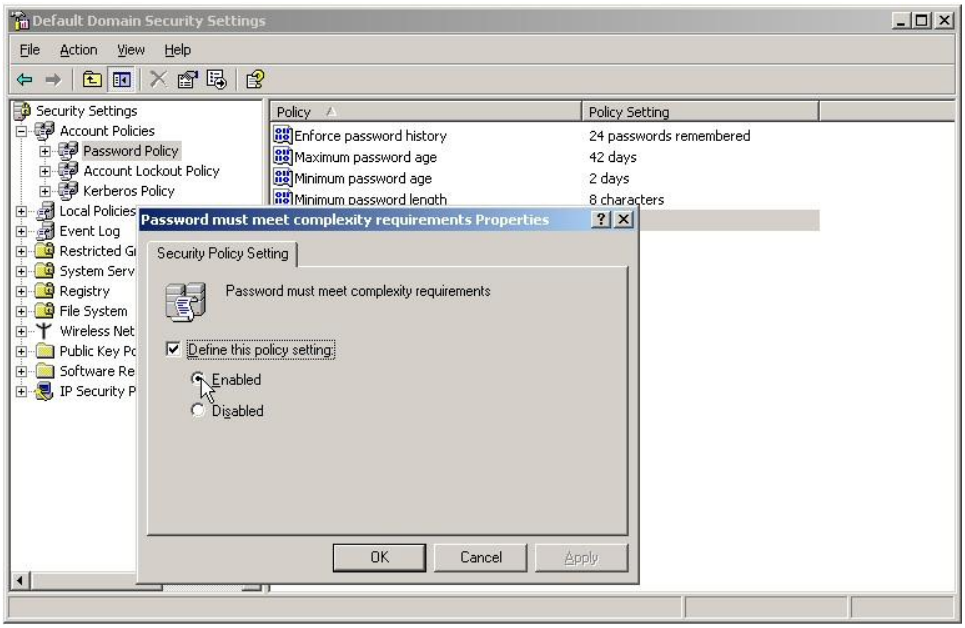
Copyright © 2008 Microsoft Corporation.

All rights reserved.

user account. For example, the strong password filter requires that passwords contain characters from at least three (3) of the following four (4) classes:

Description	Examples
1. English Upper Case Letters	A, B, C, … Z
2. English Lower Case Letters	a, b, c, … z
3. Westernized Arabic Numerals	0, 1, 2, … 9
4. Non-alphanumeric ("special characters")	For example, !,$,#,%).

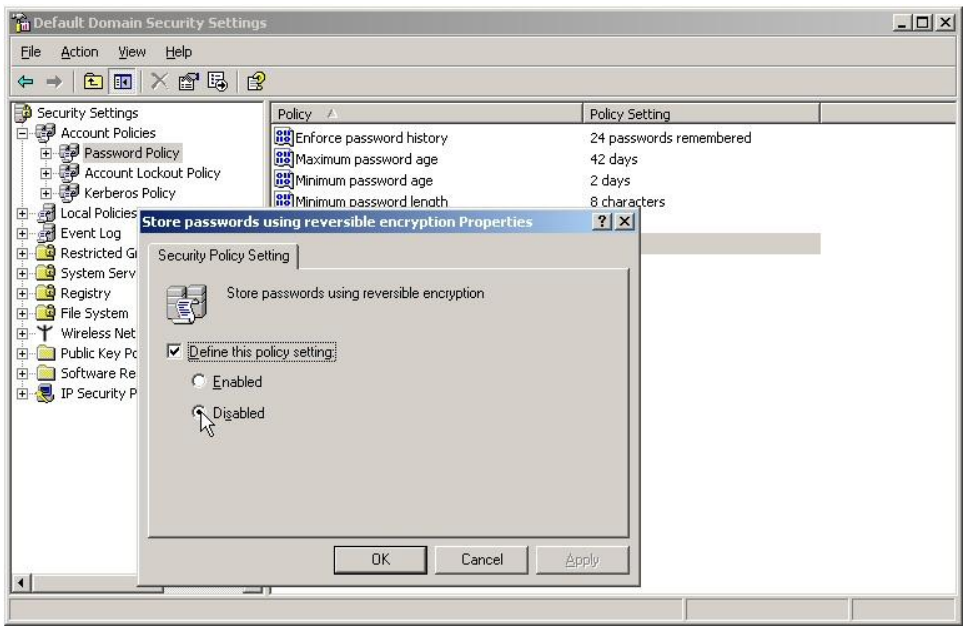
In addition, the **Passwords Must Meet Complexity Requirements** policy setting in Windows Server 2003 requires a password that is six characters or greater in length and does not allow passwords that contain the user's account name.



- **Store Password Using Reversible Encryption:** Passwords in the password database are encrypted. This encryption cannot normally be reversed. If there is a need to allow the encryption to be reversed, enable **Store password using reversible encryption for all users in the domain**. Passwords are then stored with reversible encryption and can be recovered in case of emergency. By default, this feature is disabled. This feature ***must not be enabled*** for the Windows Server 2003 Evaluated Configuration.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Configuring Account Lockout Policies

Account lockout policies control how and when accounts are locked out of the domain or the local system. By default on stand-alone servers, the **Account lockout duration** and **Reset account lockout counter after** policies are inactive, as shown below, and cannot be set until the **Account lockout threshold** policy is first changed to a value greater than zero.

To access and configure **Account Lockout Policy** settings:

1. Log on as an authorized administrator.

   Note: The examples that follow illustrate use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

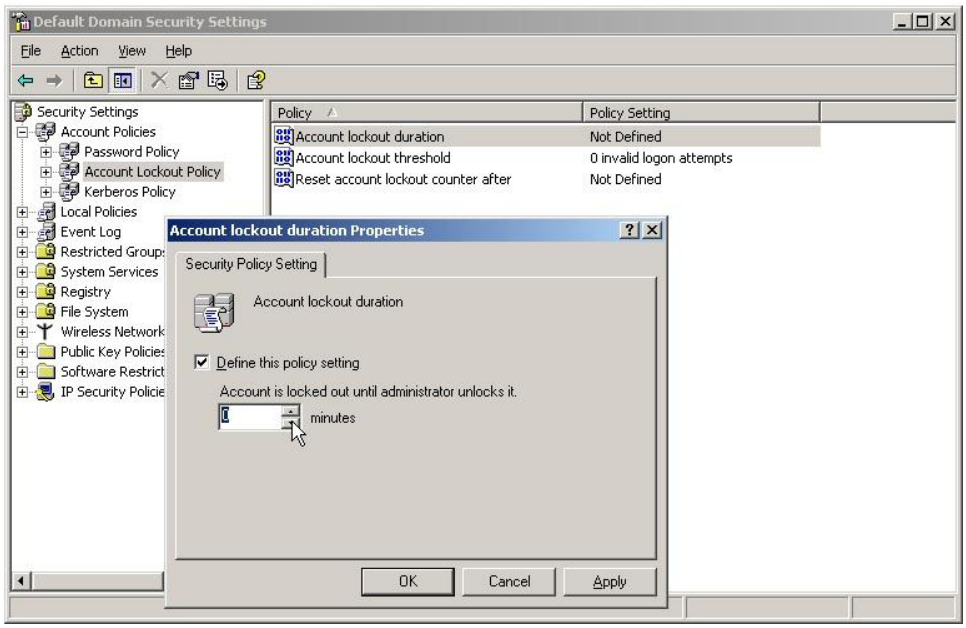
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the Default Domain Security Settings interface.
3. Expand **Account Policies** and select **Account Lockout Policy**. The configurable policy settings are presented in the right-hand details pane.
4. To edit an **Account Lockout Policy** setting, double-click on the policy setting or right-click it and select **Properties**.

These policies are described and implemented as follows:

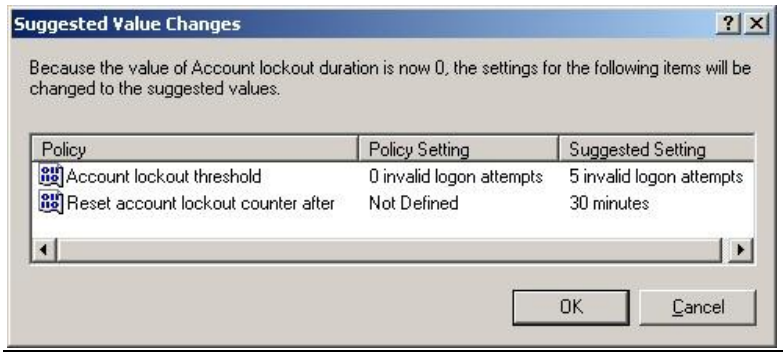
Copyright © 2008 Microsoft Corporation.
All rights reserved.

- **Account Lockout Duration.** The **Account lockout duration** policy determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from one (1) through 99,999 minutes. A value of zero (**0)** specifies that the account will be locked out until an administrator explicitly unlocks it. If **Account lockout threshold** is set to a number greater than zero, **Account lockout duration** must be greater than or equal to the value of **Reset account lockout counter after**.

  The best security policy is to require an administrator to unlock the account by setting the lockout duration to zero (0). This will block further hacker attempts to try to access the system at a later time and will force users who are locked out to seek help from an administrator, which is usually a good idea. This gives administrators the opportunity to check audit logs to determine if unauthorized login attempts were made. By talking to the user, the administrator can also determine if the user is doing anything wrong and can help the user avoid further problems.



Note: When the **Account lockout duration** policy is set first in a domain-level policy, a message will appear indicating that the settings for the **Account lockout threshold** and the **Reset account lockout counter after** policies will be automatically changed to Microsoft suggested values of five (5) invalid logon attempts and 30 minutes respectively. Click **OK** to continue. This will enable the two policies and allow them to be modified as needed.



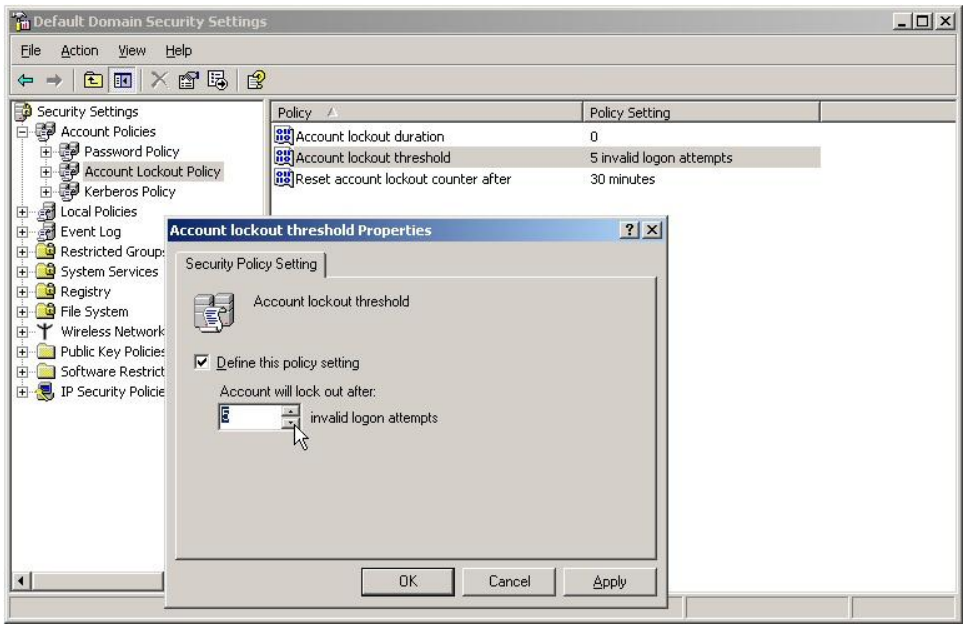
- **Account Lockout Threshold:** The **Account lockout threshold** policy sets the number of invalid logon attempts that are allowed before an account is locked out. If lockout controls are used they

Copyright © 2008 Microsoft Corporation.
All rights reserved.

should be set to a value that balances the need to prevent account cracking against the needs of users who are having difficulty accessing their accounts.

A primary reason users may not be able to access their accounts properly the first time is that they forgot their passwords. If this is the case, it may take them several attempts to log on properly. Workgroup users could also have problems accessing a remote system where their current passwords do not match the passwords the remote system expects. If this happens, several bad logon attempts may be recorded by the remote system before the user ever gets a prompt to enter the correct password. The reason is that Windows Server 2003 may attempt to automatically log on to the remote system. In a domain environment, this normally does not occur.

The lockout threshold can be set to any value from zero (0) to 999. If the lockout threshold is set to zero (0), accounts will not be locked out due to invalid logon attempts. Any other value sets a specific lockout threshold. Keep in mind that the higher the lockout value, the higher the risk that a hacker may be able to break into a system.



Note: When the **Account lockout threshold** policy is set first (in a stand-alone server Local Security Policy or a domain-level security policy), a message will appear indicating that the settings for the **Account lockout duration** and the **Reset account lockout counter after** policies will be automatically changed to Microsoft suggested values of 30 minutes each. Click **OK** to continue. This will enable the two policies and allow them to be modified as needed.

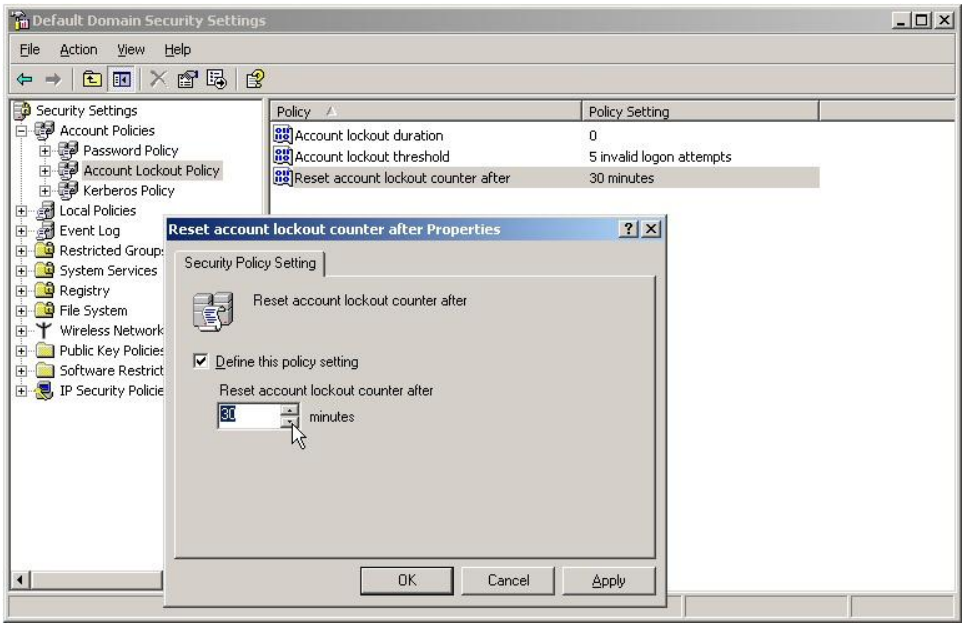
- **Reset Account Lockout Threshold After:** Every time a logon attempt fails, Windows Server 2003 raises the value of a threshold that tracks the number of bad logon attempts. The **Reset account**

Copyright © 2008 Microsoft Corporation.

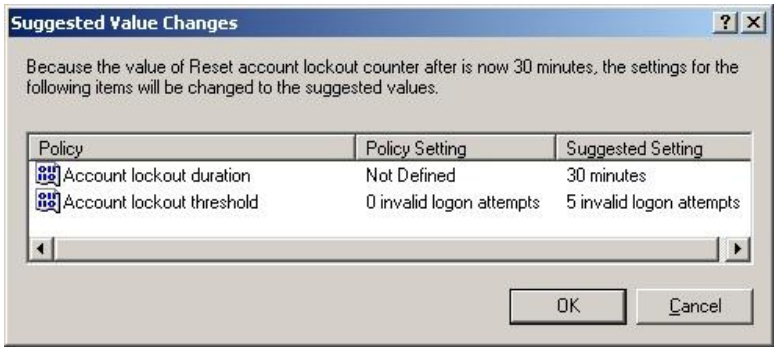
All rights reserved.

lockout threshold after policy determines how long the lockout threshold is maintained. This threshold is reset in one of two ways. If a user logs on successfully, the threshold is reset. If the waiting period for **Reset account lockout threshold after** has elapsed since the last bad logon attempt, the threshold is also reset.

By default, the lockout threshold is maintained for one minute, but any value can be set from one (1) to 99,999 minutes. As with **Account lockout threshold**, select a value that balances security needs against user access needs. A good value is from one to two hours. This waiting period should be long enough to force hackers to wait longer than they want to before trying to access the account again.



Note: When the **Reset account lockout counter after** policy is set first in a domain-level policy, a message will appear indicating that the settings for the **Account lockout duration** and the **Account lockout threshold** policies will be automatically changed to Microsoft suggested values of 30 minutes and five (5) invalid logon attempts respectively. Click **OK** to continue. This will enable the two policies and allow them to be modified as needed.



Bad logon attempts to a workstation against a password-protected screen saver do not increase the lockout threshold. Similarly, if a server or workstation is locked using **Ctrl+Alt+Delete**, bad logon attempts against the Unlock interface do not count.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Unlocking a User Account

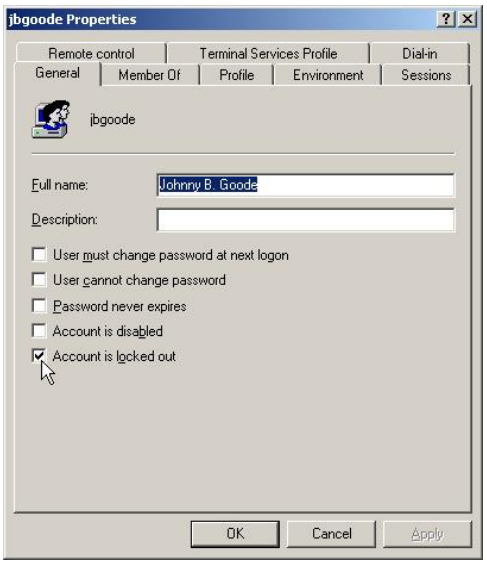
Once an account lockout threshold has been set, user accounts will be locked immediately after executing the specified number of invalid login attempts. Initial invalid login attempts will be presented to the user in a **Logon Message** as shown below.

The final invalid login attempt will inform the user that the account has been locked by presenting the **Logon Message** shown below.

An authorized administrator can unlock a local user account on a stand-alone server as follows:

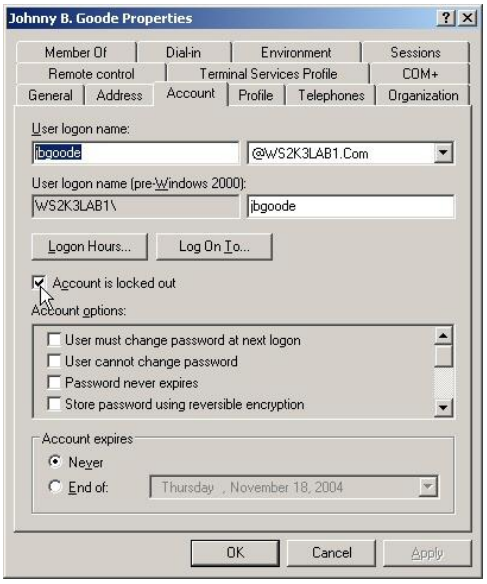
1. Click on **Start**, point to **Administrative Tools**, and then select **Computer Management**.
2. Expand **Local Users and Groups**, and then select the **Users** folder.
3. Find the account that is locked in the right-hand details pane. Double-click, or right-click, on the account and select **Properties**.
4. In the user **Properties** interface, select the **General** tab.
5. Remove the check mark from the **Account is locked out** selection box, and click on the **Apply** button.
6. Click on the **OK** button to close the user **Properties** interface.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



An authorized administrator can unlock a user account in a Windows Server 2003 domain as follows:

1. Click on **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
2. In the console tree, expand the domain node.
3. Find the user account from the appropriate organizational unit, right-click on the user account, and select **Properties**.
4. In the user **Properties** interface, select the **Account** tab.
5. Remove the check mark from the **Account is locked out** selection box, and click on the **Apply** button.
6. Click on the **OK** button to close the user **Properties** interface.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

Configuring Kerberos Policies

In Windows Server 2003, the Kerberos version 5 authentication protocol provides the default mechanism for authentication services and the authorization data necessary for a user to access a resource and perform a task on that resource. By reducing the lifetime of Kerberos tickets, the risk of a legitimate user's credentials' being stolen and successfully used by an attacker can be reduced; however, reducing the lifetime of Kerberos tickets increase authorization overhead. In most environments, these settings should not need to be changed. In a default installation of a Windows Server 2003 Active Directory domain, the default values of these policy settings, which are applied at the domain level, are configured in the Default Domain Policy GPO.

In a Windows Server 2003 Active Directory domain, Kerberos authentication is used by both client and a server in trying to determine each other's legitimacy. Kerberos works with private key cryptography. That is, both the Kerberos-enabled client and server share a secret key. Kerberos authentication works as follows (assuming the client initiates contact with the server):

1. The client generates an authenticator that contains unique information about the client (for example, client name, client realm, the time on the client, a checksum of the data in the authenticator message, and so forth). Each authenticator is unique, because of the time information it contains.
2. The client encrypts the authenticator with its copy of the secret key.
3. The client sends the encrypted authenticator to the server.
4. The server decrypts the authenticator with its copy of the secret key.
5. The server creates its own unique authenticator, which also contains a portion of the client's authenticator. That way, the server proves to the client that it received the client's authenticator, and it was able to decrypt the message, indicating that it is the proper server that had access to the secret key.

Note that since all authenticators must be unique, they are valid one time only. Therefore, Kerberos protects the system from replay attacks. A replay attack (with normal user Identification (ID)/password authentication) can occur when if an outsider can collect authentication data off of the network and replay it to the server. Since a user ID/password combination is good for many uses, the server cannot determine if the second authentication attempt is the valid user trying to open another session, or if it is an impostor trying to break into the system. Since the user ID/password information in the replay is correct, the system will grant access to the impostor.

The secret keys used in Kerberos authentication, called session keys, are also one-time use, just as authenticators are. Kerberos has a trusted authority, called the KDC that issues keys. Each client and each server is issued a long-term key by the KDC. It is so called because the key is valid for a long time. However, this key is only used when a client or server needs to communicate with the KDC. For client-server authentication, both the client and the server have to obtain a session key from the KDC. Session keys are only good for one logon session. When the session is terminated (for whatever reason) the session key that was used is no longer valid. If the same client wants to authenticate again to the same server, they both need to ask the KDC for new session keys.

The Kerberos policy is set at the domain level and is stored in the Active Directory. This means two things: One is that a user must be a member of the Domain Administrators group to change the Kerberos policy. The other is that changes made on one Domain Controller will be replicated to the other Domain Controllers along with the normal Active Directory replication.

Ticket duration, renewal, and enforcement can be controlled by adjusting the **Kerberos Policy** settings. These policies are discussed in the subsections that follow.

Warning: Only administrators with an intimate understanding of Kerberos security should change these policies. If these policies are changed to inefficient settings, serious network problems may result. In most cases the default Kerberos policy settings work just fine. Also note that in order to maintain compliance with the Evaluated Configuration the default settings for **Enforce user logon restrictions** and **Maximum tolerance for computer clock synchronization** must not be changed

Copyright © 2008 Microsoft Corporation.

All rights reserved.

from the default, as defined in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

To access and configure **Kerberos Policy** settings:

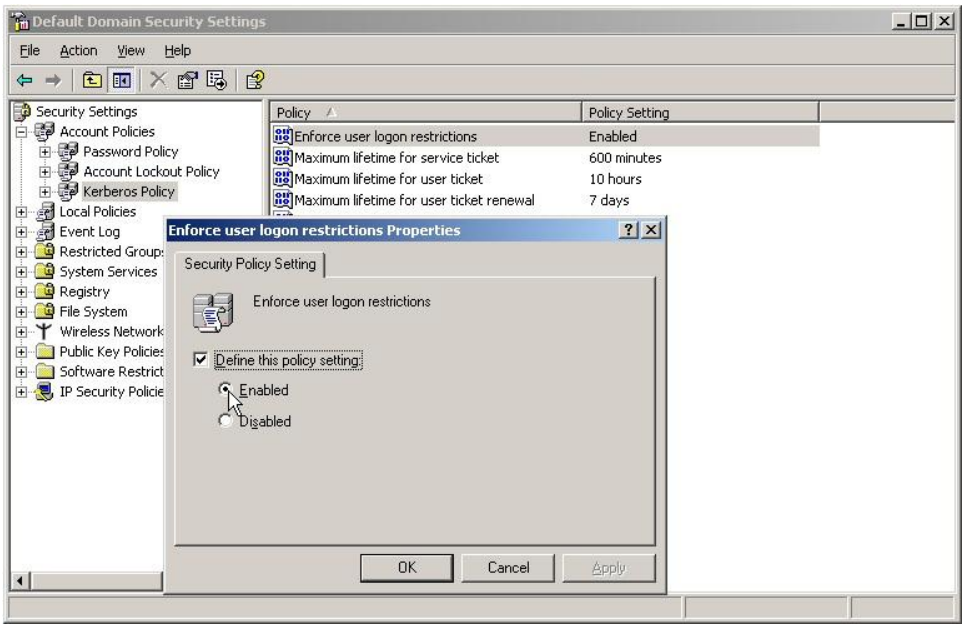
1. Log on as an authorized administrator.

Note: The examples that follow illustrate use of the **Domain** Security Policy. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Account Policies** and select **Kerberos Policy**. The configurable policy settings are presented in the right-hand details pane.
4. To edit a **Kerberos Policy** setting, double-click on the policy setting or right-click it and select **Properties**.

These policies are described and implemented as follows:

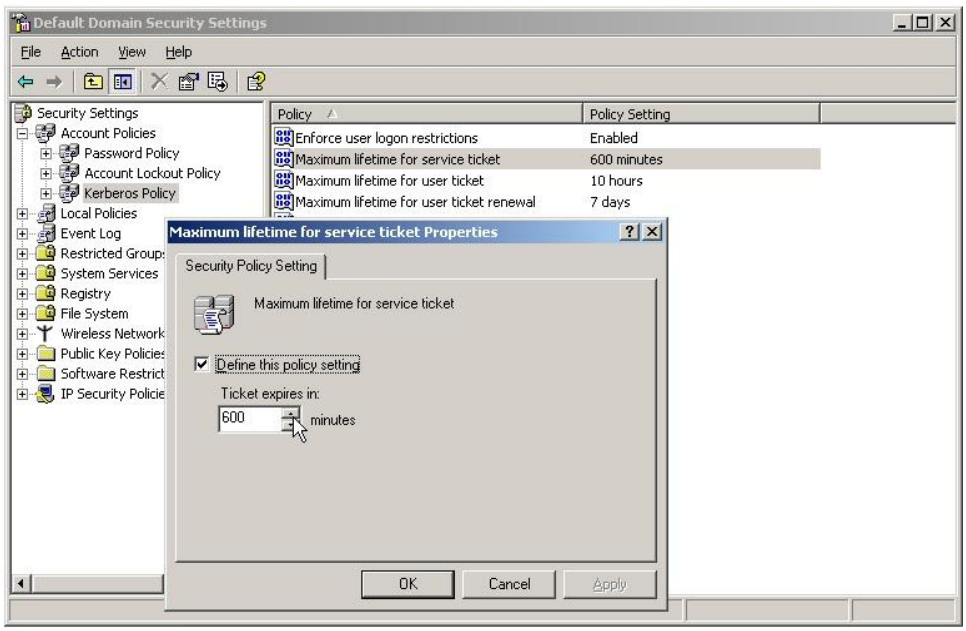
- **Enforce User Logon Restrictions:** The **Enforce user logon restrictions** policy ensures that any restrictions placed on a user account are enforced. It validates every request by checking the user rights policy to see if the user has permission to log on locally or to access the computer from the network. It also checks to make sure the account is valid. For example, if the user's logon hours are restricted, this policy is what enforces the restriction. The downside is that it may slow network access to services. By default, the policy is enabled and should only be disabled in rare circumstances.



- **Maximum Lifetime for Service Ticket:** The **Maximum lifetime for service ticket** policy is used to set the maximum duration for which a service ticket is valid. This setting determines the maximum number of minutes that a granted session ticket can be used to access a particular service. By default, service tickets have a maximum duration of 600 minutes. The duration of these tickets can be changed (although it is not recommended). The value must be 10 minutes or greater, and it must be less than or equal to the value of the **Maximum lifetime for user ticket** policy setting. A value of zero (0) effectively turns off expiration.

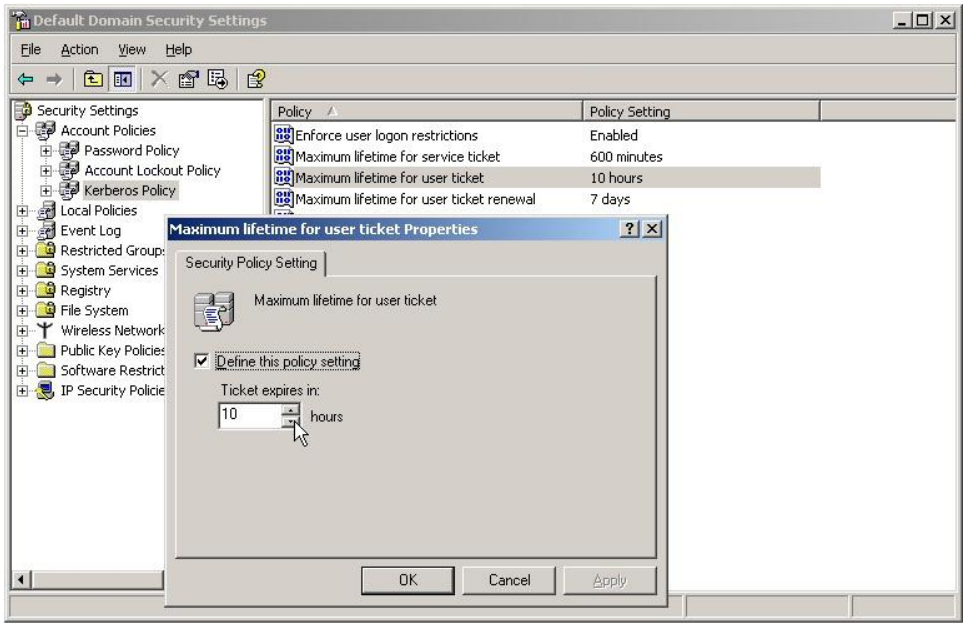
Copyright © 2008 Microsoft Corporation.

All rights reserved.



- **Maximum Lifetime for User Ticket:** The **Maximum lifetime for user ticket** policy is used to set the maximum amount of time (in hours) that a user's ticket-granting ticket can be used. By default, user tickets have a maximum duration of 10 hours. When a user's ticket-granting ticket expires, a new one must be requested or the existing one must be renewed. The duration of these tickets can be changed (although it is not recommended). For user tickets, the valid range is from zero (0) to 99,999 hours. A value of zero (0) effectively turns off expiration.

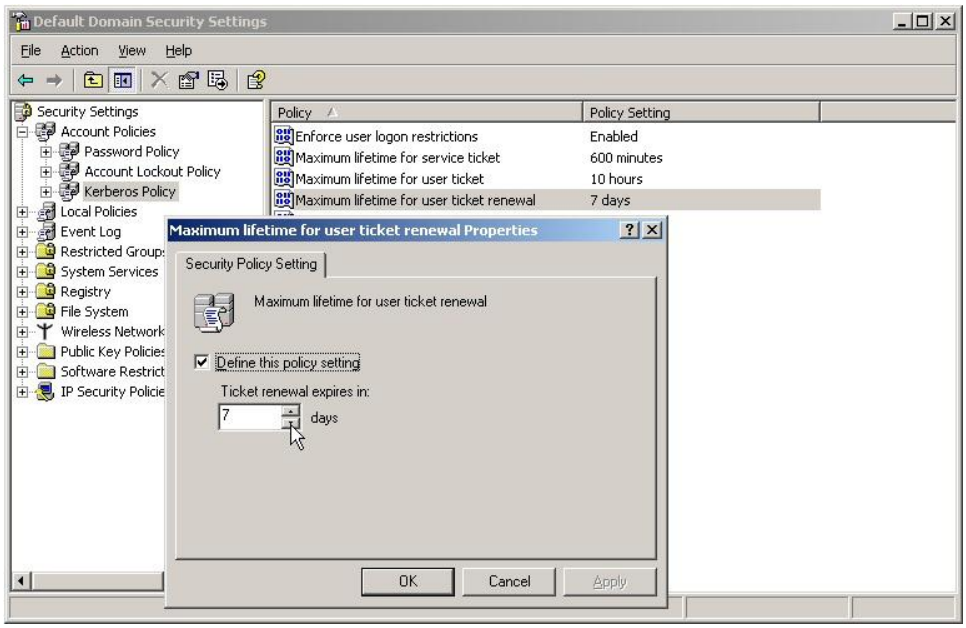
Note: If the value for this policy setting is too high, users might be able to access network resources outside of their logon hours, or users whose accounts have been disabled might be able to continue to access network services by using valid service tickets that were issued before their account was disabled. A value of zero (0) is not recommended because the ticket-granting tickets would never expire.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

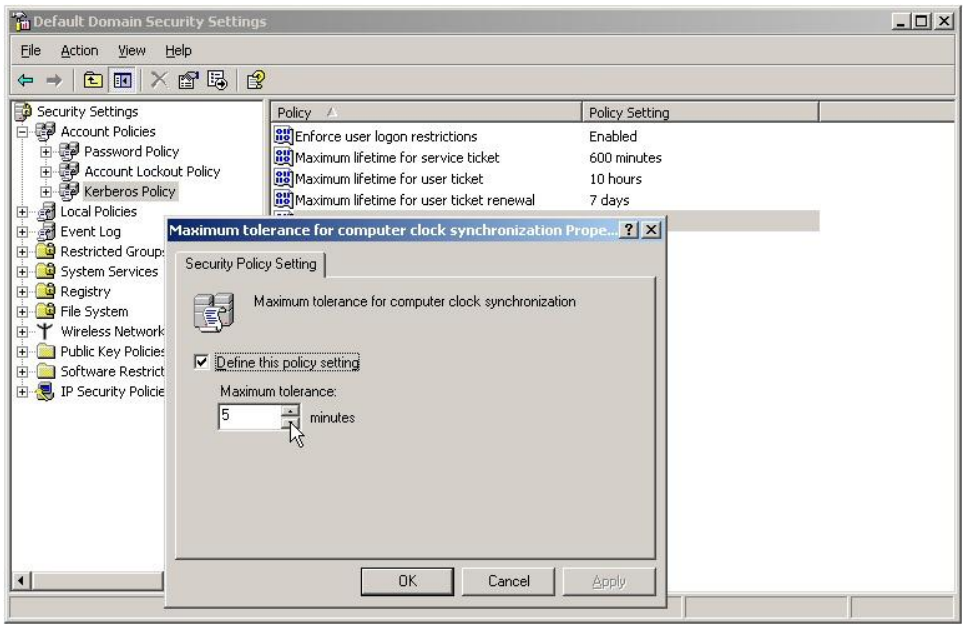
- **Maximum Lifetime for User Ticket Renewal:** A ticket that expires can be renewed, provided the renewal takes place within the time set by the **Maximum lifetime for user ticket renewal** policy. By default, the maximum renewal period is seven (7) days. The renewal period can be changed to any value from zero (0) to 99,999 days (although it is not recommended). A value of zero (0) effectively turns off the maximum renewal period.



- **Maximum Tolerance for Computer Clock Synchronization:** The **Maximum tolerance for computer clock synchronization** policy determines the maximum time difference (in minutes) that Kerberos V5 tolerates between the time on the client clock and the time on the Domain Controller running Windows Server 2003 that provides Kerberos authentication. By default, computers in the domain must be synchronized within five minutes of each other. If the client clock and the server clock are not synchronized closely enough, a client ticket is not issued. The default value is five (5) minutes. If there are remote users that log on to the domain without synchronizing their clock to the network timeserver, it may be necessary to adjust this value. However, changing this value to provide a wider margin can leave the system open to replay attacks. Therefore the default must be maintained for the Evaluated Configuration.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Local Policies

Local Policies determine the security options for a user or service account. Local policies are based on the computer a user is logged into, and the rights the user has on that particular computer. Local Policies can be used to configure:

- **Audit policy.** Determines which security events will be logged into the Security log on the computer (successful attempts, failed attempts or both). The Security log can be viewed through the Event Viewer GUI.
- **User rights assignment.** Determines which users or groups have logon or task privileges on the computer.
- **Security options.** Enables or disables security settings for the computer, such as digital signing of data, Administrator and Guest account names, floppy drive and CD ROM access, driver installation, and logon prompts.

Local policies, by definition, are local to a computer. When these settings are imported from a GPO in Active Directory, they will affect the local security settings of any computer accounts to which that GPO is applied. Because a computer can have more than one policy setting applied to it, security policy settings can conflict with each other. The order of precedence from highest to lowest is: OU, domain, site, and local computer.

Configuring Audit Policies

Planning is an important step in the auditing process. Administrators should be selective in determining the objects to audit. Auditing creates system overhead, therefore auditing too many objects will cause the security log to become large and difficult to manage.

Before audit records are logged, an auditing policy must be established. The policy defines the types of events that will be audited for a specific user or group of users. However, enabling the auditing policy is only part of the work associated with setting up auditing. Auditing implementation has several steps:

1. Enable auditing through a **Local Security Policy** or a domain-level security policy.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

2. To support the **Audit object access** policy, select the objects to be audited, and set the System Access Control Lists (SACL) for the objects.
3. Configure the event log.
4. Protect the audit data from unauthorized access or modification.
5. Review and maintain the audit logs.

This subsection deals only with steps one and two; all other aspects of audit management are addressed in the Audit Management subsection of this document.

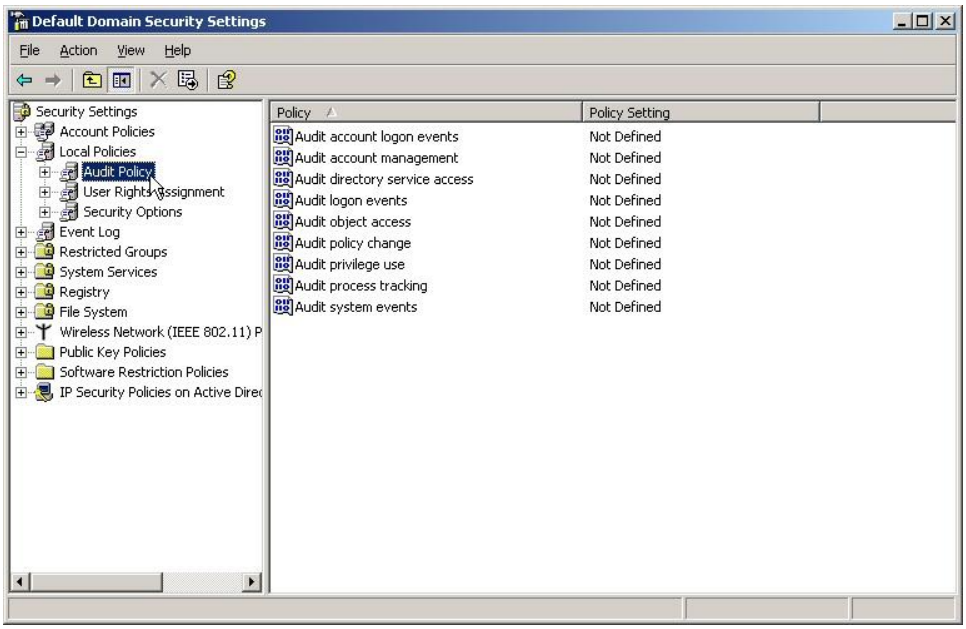
An auditing policy specifies categories of security-related events that must be audited. Windows Server 2003 has various **Audit Policy** settings enabled by default in a stand-alone server **Local Security Policy** and in a **Domain Controller Security Policy** to monitor successful actions. In a **Domain Security Policy** audit policies are **Not Defined** by default. By turning on various auditing event categories to monitor successes and/or failures, the administrator can tailor an auditing policy that suits the security needs of the organization.

To enable or disable audit, access and edit the **Audit Policy** settings as follows:

1. Log on using an authorized administrator.

Note: The examples that follow illustrate use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

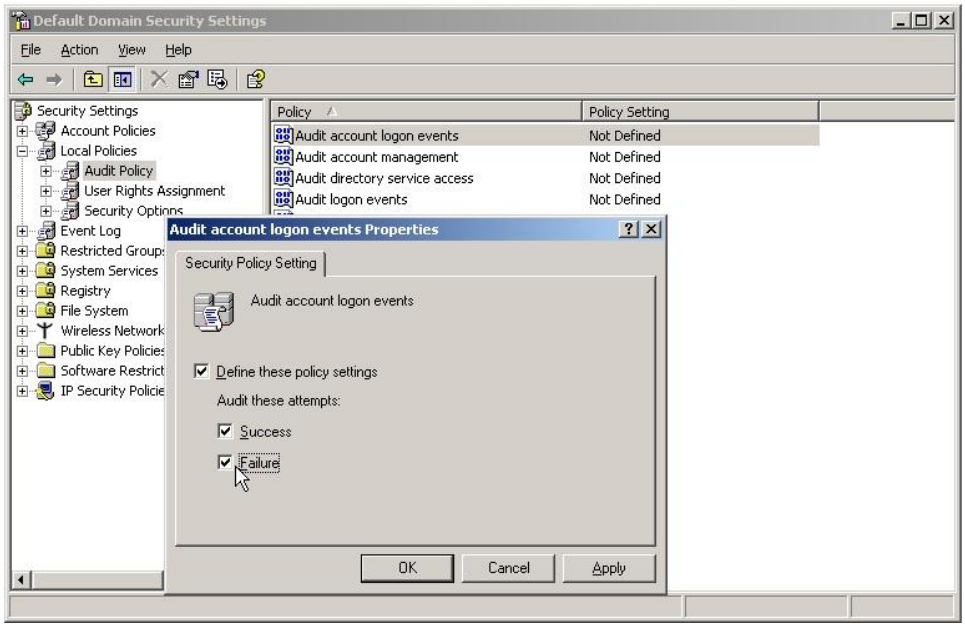
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand Local Policies and select **Audit Policy**. The configurable audit event categories are presented in the right-hand details pane.



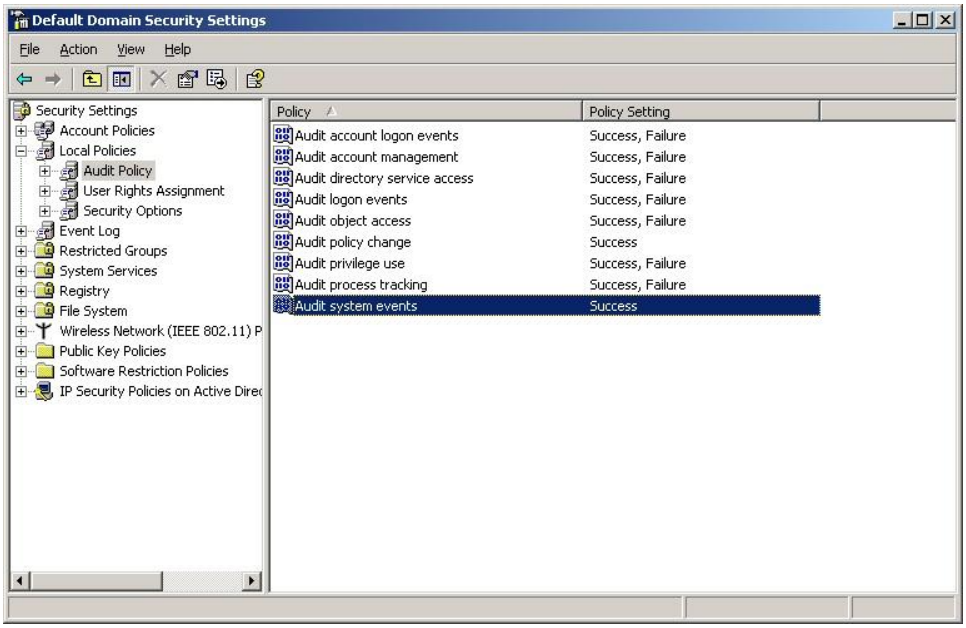
4. To set an audit policy, double-click on an audit event category. For domain-level policies, check the **Define these policy settings** check box and then check the appropriate boxes to select whether to enable audit **Success** and/or **Failure** events for this category. To disable the auditing of a **Success** or **Failure** in any of the audit categories, simply uncheck the corresponding box.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. Click **OK**. Repeat the process for other audit categories. It will take a few minutes for the change to take effect, and other Domain Controllers will receive the change at the next regular replication interval.



Best Practices for Auditing

To minimize the risk of several specific security threats, the administrator can take various auditing steps. The administrator should select the events to be audited considering the set of threats specific to the environment. The following table provides an example of various events that could be audited, as well as the specific security threat that the audit event monitors.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Audit Event	Potential Threat
Failure audit for logon/logoff	Random password hack
Success audit for logon/logoff	Stolen password break-in
Success audit for user rights, user and group management, security change policies, restart, shutdown, and system events	Misuse of privileges
Success and failure audit for file-access and object-access events. File Manager success and failure audit of Read/Write access by suspect users or groups for the sensitive files.	Improper access to sensitive files
Success and failure audit for file-access printers and object-access events. Print Manager success and failure audit of print access by suspect users or groups for the printers.	Improper access to printers
Success and failure write access auditing for program files (Execute (.EXE) and Dynamic Link Library (.DLL) extensions). Success and failure auditing for process tracking. Run suspect programs; examine security log for unexpected attempts to modify program files or create unexpected processes. Run only when actively monitoring the system log.	Virus outbreak

Appendix B – Audit Categories and Events, of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*, contains a table that provides a cross reference of audit categories and audit events to the auditable events required in the Windows XP/Server 2003 ST requirements. This can be used as a reference when implementing an audit policy that must address specific ST requirements.

Enabling Object Auditing

If audit access to objects is chosen as part of the audit policy, either the audit directory service access category (for auditing objects on a Domain Controller), or the audit object access category (for auditing objects on a member server) must be also turned on. Once the correct object access category has been turned on, each individual object's **Properties** can be used to specify whether to audit successes or failures for the specific access request to each group or user.

Enabling Auditing on Directory Objects

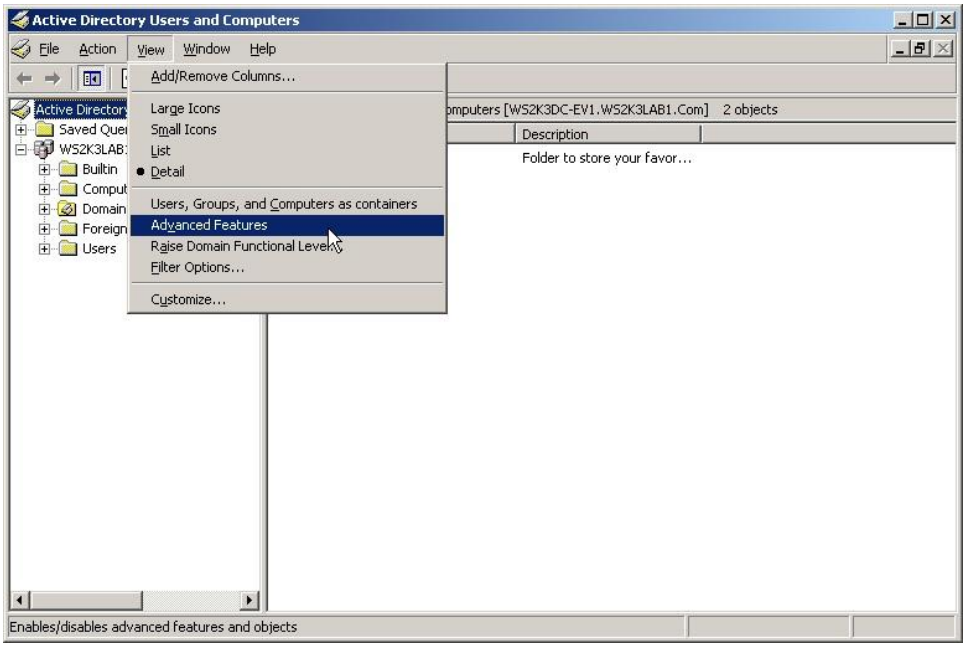
The administrator can set an auditing SACL for an Active Directory object using the following procedure:

Warning: The **Manage auditing and security log** privilege (SeSecurityPrivilege) allows a user to set SACLs on objects. Administrators must ensure that this privilege is not assigned to non-administrative user accounts.

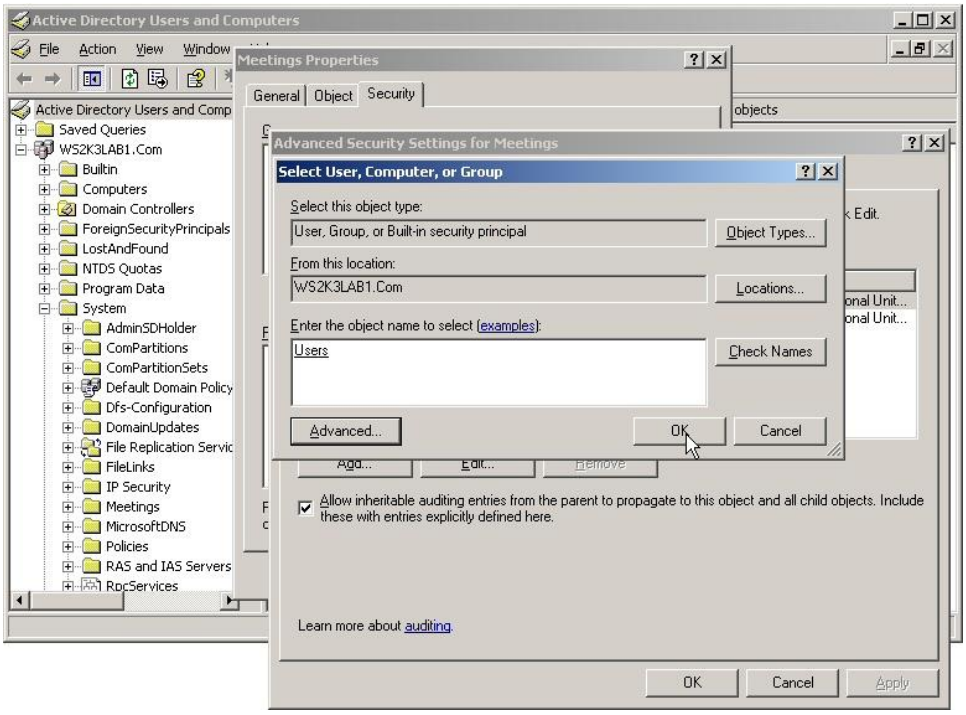
1. Log on using an authorized administrator for the domain.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. On the **View** menu, select **Advanced Features**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



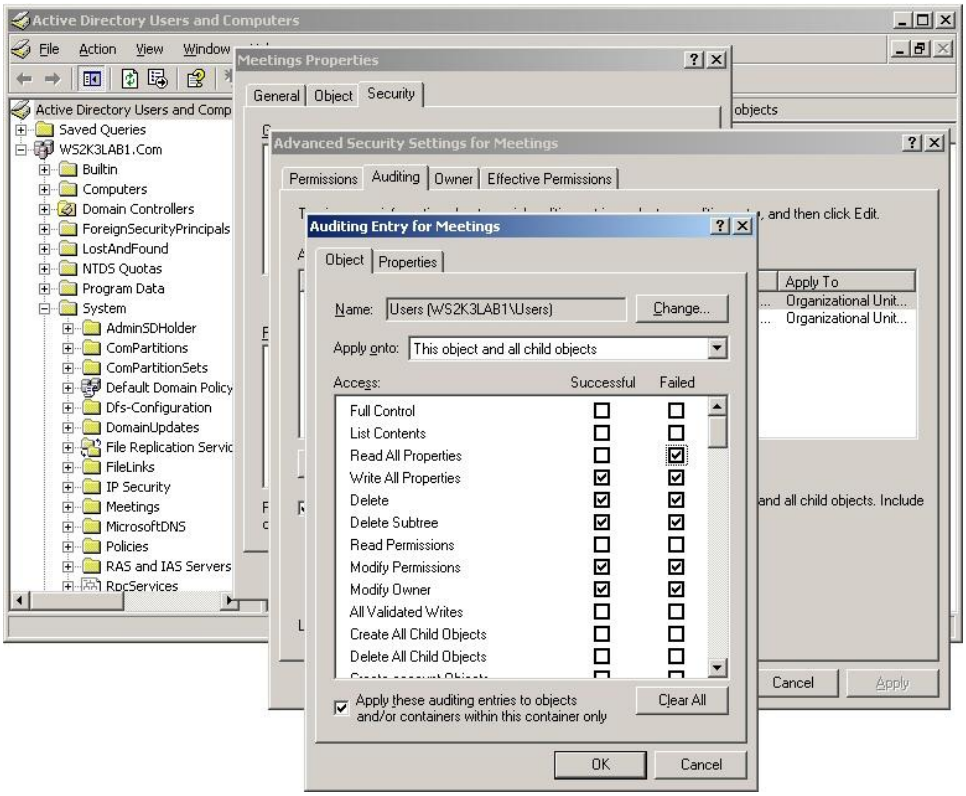
4. Locate the container for the object, right-click it, and then click **Properties**.
5. Click the **Security** tab.
6. Click **Advanced**, and click the **Auditing** tab.
7. Click the **Add** button.
8. In **Select User, Computer, or Group**, type the account name, or click **Advanced** and then **Find Now** to select a user from the list, and then click **OK** to automatically open the **Auditing Entry** interface.



9. The **Auditing Entry** interface has two tabs—**Object** and **Properties**.
10. The **Object** tab allows the selection of generic and control rights to audit.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

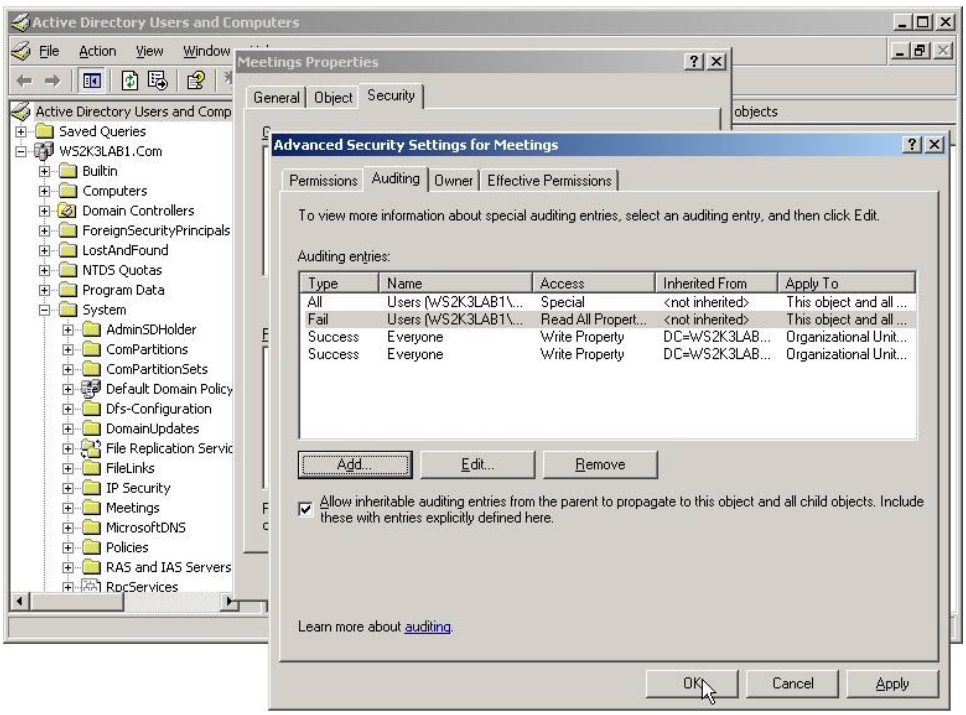
11. The **Properties** tab allows selection of property accesses to audit.
12. Use the pull-down lists to make selections on the types of object on which the settings will be applied.
13. Click each tab that needs to be modified, and select the check boxes for the successful or failed access actions to be audited.
14. Check the **Apply…** box and then click **OK**.



15. In the **Advanced Security Settings** interface, choose whether the choices will be inherited from the parent container to this object. If yes, then select the **Allow inheritable auditing entries from parent to propagate to this object and all child objects** check box.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



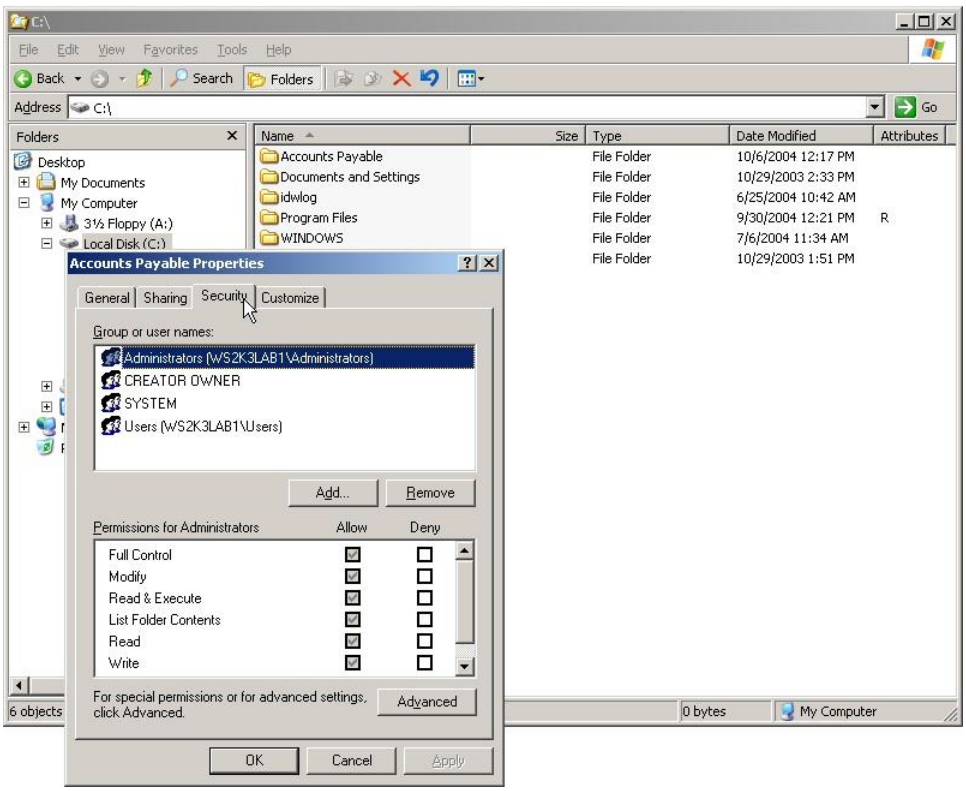
16. Click **Apply**, and then click **OK** on the **Advanced Security Settings** interface.
17. Click **OK** on the container **Properties** interface.

Enabling and editing Audit on Files and Folders

To set, view, modify, or remove auditing for a file or folder:

1. Open **Windows Explorer**, and then locate the file or folder to audit.
   - Click **Start** and select **Windows Explorer**; or
   - Click **Start** and select **My Computer**.
2. Navigate **Windows Explorer** to find the file or folder object where auditing is to be set. Right-click the file or folder, select **Properties**, and then click the **Security** tab.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



3. Click **Advanced**, and then click the **Auditing** tab.
4. To audit actions against the object by a user or group, click **Add**.

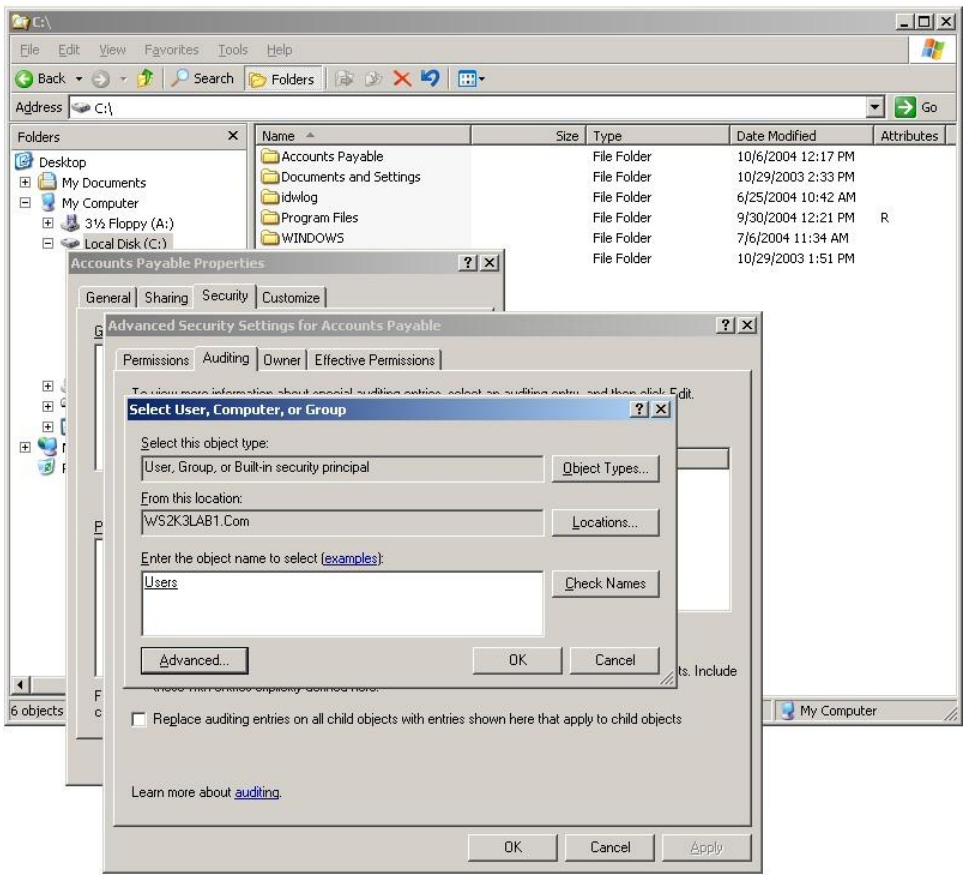
Note: By default, audit is not set on files and folders. Therefore the **Auditing entries** box will initially show no accounts.

---

5. In the **Select User or Group** interface, type the user or group name, or click **Advanced** and then **Find Now** to select a user or group from the list, and then click **OK** to automatically open the **Auditing Entry** interface.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



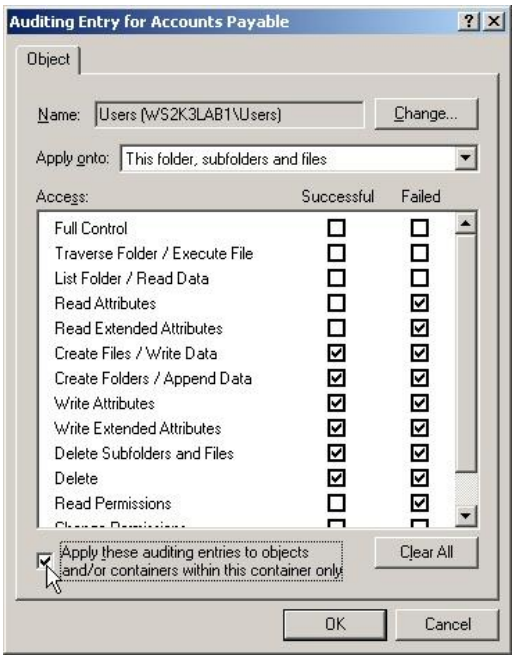
6. In the **Auditing Entry** interface, under **Access** click **Successful**, **Failed**, or both to select the events to be audited for this user or group. If necessary, check the **Apply these auditing entries to objects and/or containers within this container only** selection box. See "Selecting where to apply auditing entries on files and folders" for details on how the **Apply these auditing entries to objects and/or containers within this container only** selection box impacts the propagation of changes to sub-containers. The table below provides a description of the file and folder access events that may be audited.

Select	To audit
Full Control	All attempts to access a folder or file.
Traverse Folder / Execute File	Any attempts to move through folders to reach other folders or files.
List Folder / Read Data	Any attempts to view file names and subfolder names within a folder.
Read Attributes	Any attempts to view the attributes of a file or folder, such as the "Read-only" and "Hidden" attributes.
Read Extended Attributes	Any attempts to view the extended attributes of a file or folder. Extended attributes are defined by programs and may vary by program.
Create Files / Write Data	Any attempts to create files within a folder.
Create Folders / Append Data	Create folder audits any attempts to create folders within the folder. Append data audits any attempts to make changes to the end of a file but not changing, deleting, or overwriting existing data.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Select	To audit
Write Attributes	Any attempts to change the attributes of a file or folder, such as the "Read-only" and "Hidden" attributes.
Write Extended Attributes	Any attempts to change the extended attributes to a file or folder. Extended attributes are defined by programs and may vary by program.
Delete Subfolders and Files	Any attempts to delete subfolders and files.
Delete	Any attempts to delete the file or folder.
Read Permissions	Any attempts to read the file or folder.
Change Permissions	Any attempts to change the permissions of the file or folder.
Take Ownership	Any attempts to take ownership of a file or folder.

7. Click **OK** to close the **Auditing Entry** interface.



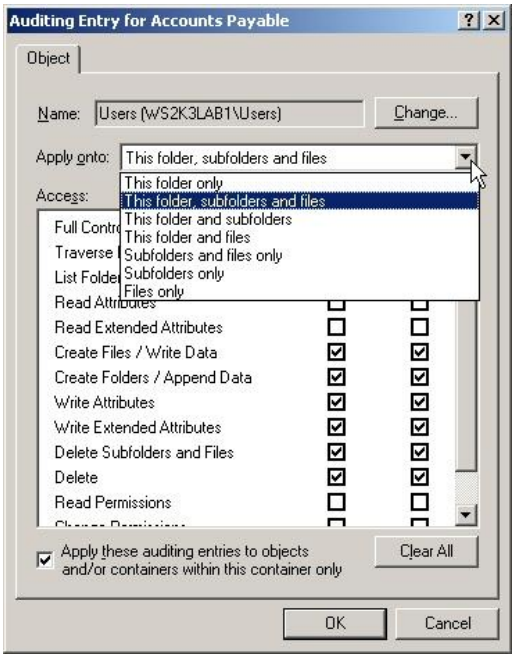
8. To view or change auditing for an existing group or user, simply select on the name, and then click the **Edit** button.
9. To remove auditing for an existing group or user, select the name, and then click the **Remove** button.

Note: Before Windows Server 2003 will audit access to files and folders, the **Audit Object Access** setting in the **Audit Policy** must be enabled. If not, an error message will appear when auditing is set up for files and folders, and no files or folders will be audited. Once auditing is enabled, view the security log in **Event Viewer** to review successful or failed attempts to access the audited files and folders.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Selecting Where to Apply Auditing Entries on Files and Folders

The **Auditing Entry** interface appears when setting audit on files and folders. In this interface, the **Apply onto** list displays the locations where auditing entries can be applied. How these auditing entries are applied depends on whether **Apply these auditing entries to objects and/or containers within this container only** is selected. By default, this check box is cleared.



When the **Apply these auditing entries to objects and/or containers within this container only** check box is clear, audit settings are applied as shown below:

Apply onto	Audits current folder	Audits subfolders in the current folder	Audits files in the current folder	Audits all subsequent subfolders	Audits files in all subsequent subfolders
This folder only	✓				
The folder, subfolders and files	✓	✓	✓	✓	✓
This folder and subfolders	✓	✓		✓	
This folder and files	✓		✓		✓
Subfolders and files only		✓	✓	✓	✓
Subfolders only		✓		✓	
Files only			✓		✓

When the Apply these auditing entries to objects and/or containers within this container only check box is selected, audit settings are applied as shown below:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Apply onto	Audits current folder	Audits subfolders in the current folder	Audits files in the current folder	Audits all subsequent subfolders	Audits files in all subsequent subfolders
This folder only	✓				
The folder, subfolders and files	✓	✓	✓		
This folder and subfolders	✓	✓			
This folder and files	✓		✓		
Subfolders and files only		✓	✓		
Subfolders only		✓			
Files only			✓		

Enabling Auditing of IPSec Data Integrity Violations and Replay of TFS Data

Starting with Windows Server 2003 SP1, the ability to audit IPSec data integrity violations and data replay attempts was added. To enable this audit the Audit System Events category in the Local Security Policy or Domain-level security policies must be set to detect Failure. See the Configuring Audit Policies subsection for details on how to set auditing of system events. In addition, to enable this capability, it will be necessary edit the Registry to create and set the value of the Registry entry shown below. For examples on editing the Registry, see the Configuring Security Target Requirements through the Registry Editor subsection.

Key Path: **HKLM\SYSTEM\CurrentControlSet\Control\Lsa**		**Format**	**Value**
Key: Audit	**Value Name:** ReplayIntegrityLogging	REG_DWORD	1

Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Enabling and Editing Audit on Registry Keys

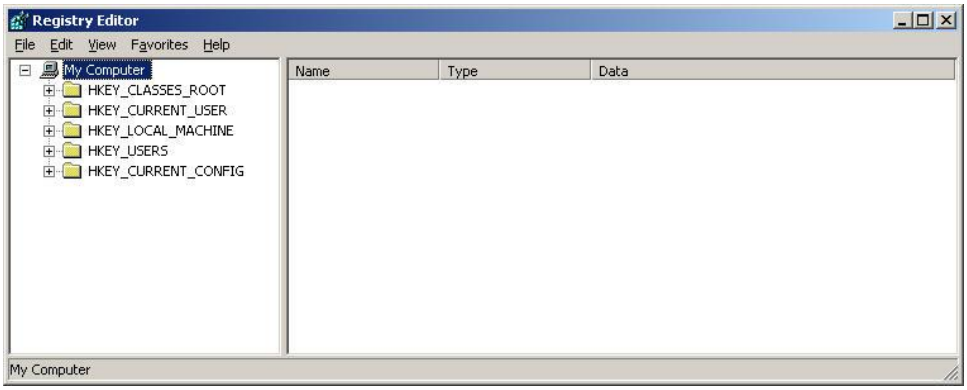
Auditing of Registry keys may be used to monitor attempts to modify system configuration settings or to troubleshoot problems that may result from application installations. To set, view, modify, or remove auditing for a Registry key:

Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

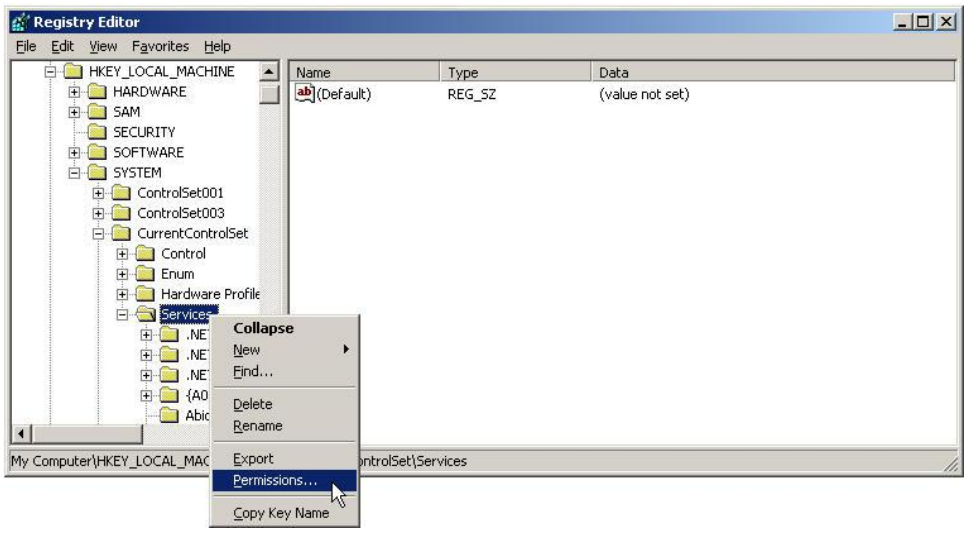
1. Log on as an authorized administrator.
2. Open the Registry Editor:
   - Click **Start** and select **Run**; then

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Type **regedit** in the **Open** text box and click **OK** to open the **Registry Editor**.



3. Navigate to the Registry path where the desired key is located.
4. Right-click on the desired Registry key and select **Permissions**.



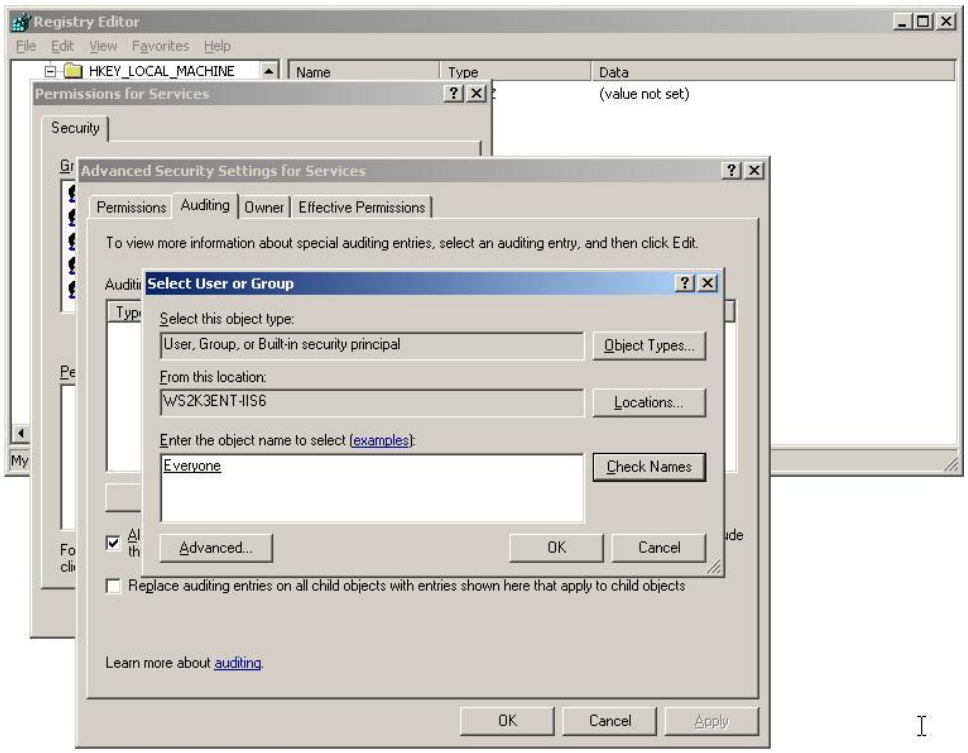
5. Click the **Advanced** button on the **Permissions for <registry key>** interface, and then click the **Auditing** tab on the **Advanced Security Settings for <registry key>** interface.
6. To set audit access to the Registry key by a user or group, click **Add**.

Note: By default, audit is not set on Registry keys. Therefore, the **Auditing entries** box will initially show no accounts.

---

7. In the **Select User or Group** interface, type the user or group name, or click **Advanced** and then **Find Now** to select a user or group from the list, and then click **OK** to automatically open the **Auditing Entry for <registry key>** interface.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

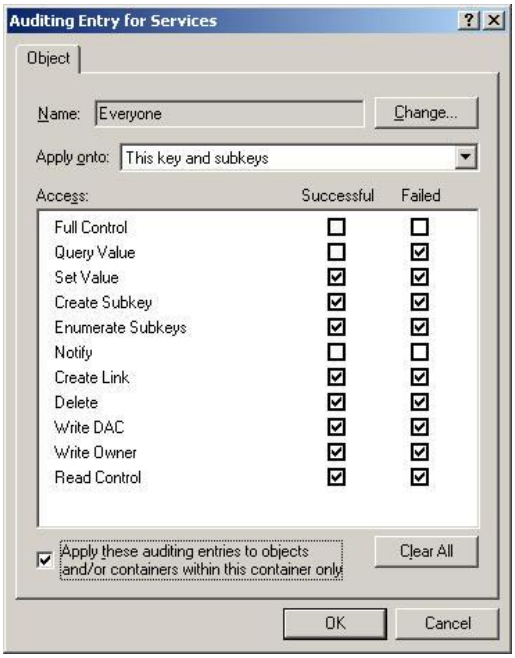


8. In the **Auditing Entry** interface, under **Access,** click **Successful**, **Failed**, or both to select the events to be audited for this user or group. If necessary, check the **Apply these auditing entries to objects and/or containers within this container only** selection box. See Selecting where to apply auditing entries on Registry keys and subkeys for details on how the **Apply these auditing entries to objects and/or containers within this container only** selection box impacts the propagation of changes to subkeys. The table below provides a description of the Registry access events that may be audited.

Select	To audit
Full Control	All attempts to access an entry from a registry key.
Query Value	Any attempts to read an entry from a registry key.
Set Value	Any attempts to set entries in a registry key.
Create Subkey	Any attempts to create subkeys on a selected registry key.
Enumerate Subkeys	Any attempts to identify the subkeys of a registry key.
Notify	Any notification events from a key in the registry.
Create Link	Any attempts to create a symbolic link in a particular key.
Delete	Any attempts to delete a registry object.
Write DAC	Any attempts to write a discretionary access control list on the key.
Write Owner	Any attempts to change the owner of the selected key.
Read Control	Any attempts to open the discretionary access control list on a key.

9. Click **OK** to close the **Auditing Entry** interface.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



10. To view or change auditing for an existing user or group, select the name from the **Auditing entries** box of the **Auditing** tab view, and then click **Edit**.
11. To remove auditing for an existing user or group, select the name, and then click **Remove**.

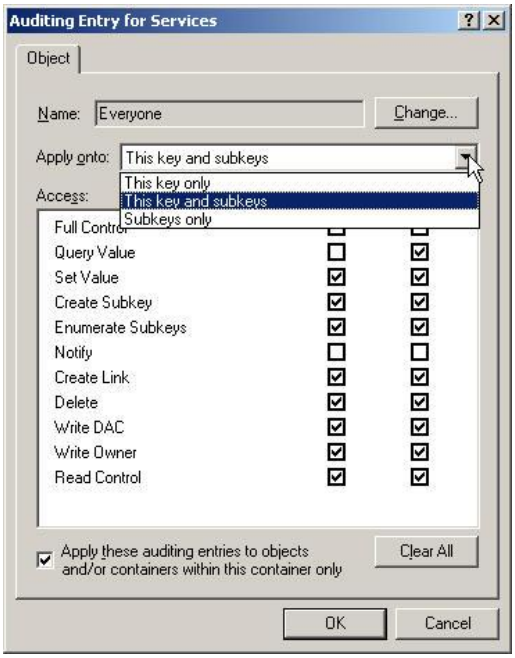
Note: Before Windows Server 2003 will audit access to Registry keys and subkeys, the **Audit Object Access** setting in the **Audit Policy** must be enabled. If not, an error message will appear when auditing is set up for keys and subkeys, and no keys or subkeys will be audited. Once auditing is enabled, view the security log in Event Viewer to review successful or failed attempts to access the audited keys and subkeys.

Selecting Where to Apply Auditing Entries on Registry Keys and Subkeys

The **Auditing Entry** interface appears when setting audit on files and folders or on Registry keys. In this dialog box, the **Apply onto** list displays the locations where auditing entries can be applied. How these auditing entries are applied depends on whether **Apply these auditing entries to objects and/or containers within this container only** is selected. By default, this check box is cleared.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



When the **Apply these auditing entries to objects and/or containers within this container only** check box is clear, audit settings are applied as shown below:

Apply onto	Audits current key	Audits subkeys in the current key	Audits all subsequent subkeys
This key only	✓		
This key and subkeys only	✓	✓	✓
Subkeys only		✓	✓

When the **Apply these auditing entries to objects and/or containers within this container only** check box is selected, audit settings are applied as shown below:

Apply onto	Audits current key	Audits subkeys in the current key	Audits all subsequent subkeys
This key only	✓		
This key and subkeys only	✓	✓	
Subkeys only		✓	

Configuring User Rights

Although the built-in capabilities for accounts cannot be changed, user rights for accounts can be administered. These rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories. User rights are different from permissions because they apply to user accounts, whereas permissions are attached to objects. Keep in mind that changes made to

Copyright © 2008 Microsoft Corporation.
All rights reserved.

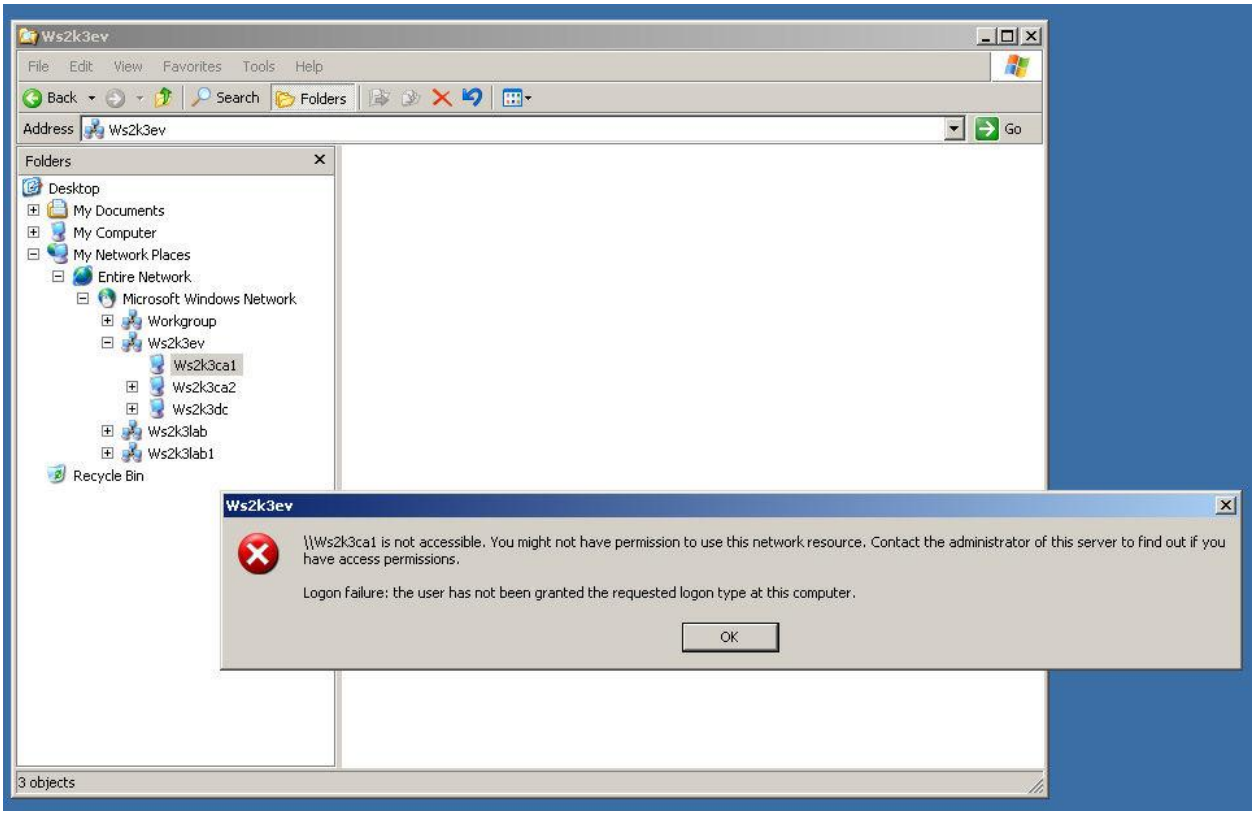
user rights can have a far-reaching effect. Because of this, only experienced administrators should make changes to the user rights policy.

Microsoft defines user rights in two types of categories: Logon Rights and Privileges. These are defined as follows:

- **Logon Right:** A user right that is assigned to a user and that specifies the ways in which a user can log onto a system. An example of a logon right is the right to log on to a system remotely.
- **Privilege:** A user right that is assigned to a user and that specifies allowable actions on the system. An example of a privilege is the right to shut down a system.

User rights define capabilities at the local level. Although they can apply to individual user accounts, user rights are best administered on a group account basis. This ensures that a user logging on as a member of a group automatically inherits the rights associated with that group. By assigning rights to groups rather than individual users, user account administration can be simplified. When users in a group all require the same user rights, they can be assigned the set of rights once to the group, rather than repeatedly assigning the same set to each individual user account.

User rights that are assigned to a group are applied to all members of the group while they remain members. If a user is a member of multiple groups, the user's rights are cumulative, which means that the user has more than one set of rights and privileges. The only time that rights assigned to one group might conflict with those assigned to another is in the case of certain logon rights. For example a member of multiple groups who is assigned the **Deny access to this computer from network** logon right on a specific computer would not be able access the computer remotely despite the logon rights granted to the user by other groups. When attempting to access resources on the remote computer, the user would receive the message shown below.



In general, however, user rights assigned to one group do not conflict with the rights assigned to another group. To remove rights from a user, the administrator simply removes the user from the group. In this case, the user no longer has the rights assigned to that group.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The following lists show the logon rights and privileges that can be assigned to a user.

Logon Rights

- Access this computer from a network
- Allow logon through Terminal Services
- Log on as a batch job
- Log on as a service
- Log on locally
- Deny access to this computer from network
- Deny local logon
- Deny logon as a batch job
- Deny logon as a service
- Deny logon through Terminal Services

Privileges

- Act as part of the operating system
- Add workstations to a domain
- Adjust memory quotas for a process
- Back up files and directories
- Bypass traverse checking
- Change the system time
- Create a token object
- Create a pagefile
- Create permanent shared objects
- Debug programs
- Enable computer and user accounts to be trusted for delegation
- Force shutdown from a remote system
- Generate security audits
- Increase scheduling priority
- Load and unload device drivers
- Lock pages in memory
- Manage auditing and security log
- Modify firmware environment values
- Profile a single process
- Profile system performance
- Remove computer from docking station
- Replace a process level token
- Restore files and directories
- Shut down the system
- Synchronize directory service data
- Take ownership of files or other objects

Some of the privileges can override permissions set on an object. For example, a user logged on to a domain account as a member of the Backup Operators group has the right to perform backup operations for all domain servers. However, this requires the ability to read all files on those servers, even files on which their owners have set permissions that explicitly deny access to all other users, including members of the Backup Operators group. A user privilege, in this case, the right to perform a backup, takes precedence over all file and directory permissions. The privileges, which can override permissions set on an object, are listed below.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Take ownership of files or other object
- Manage auditing and security log
- Back up files and directories
- Restore files and directories
- Debug programs
- Bypass traverse checking

The **Take ownership of files or other object** (TakeOwnership) privilege grants WriteOwner access to an object. **Backup** and **Restore** privileges grant read and write access to an object. The **Debug programs** (debug) privilege grants read or open access to an object. The **Bypass traverse checking** (ChangeNotify) privilege provides the reverse access on directories. This privilege is given, by default, to all users and is not considered security relevant. The **Manage auditing and security log** (SeSecurityPrivilege) privilege provides several abilities including access to the security log, overriding access restrictions to the security log. The Event Logger is responsible for enforcing the Security privilege in this context. The TakeOwnership, Security, Backup, Restore, Debug privileges should only be assigned to administrator accounts (See Appendix C, User Rights and Privileges, of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*, for the restrictions of the assignment of privileges to be in accordance with the Evaluated Configuration).

The special user account LocalSystem has almost all privileges and logon rights assigned to it, because all processes that are running as part of the operating system are associated with this account, and these processes require a complete set of user rights.

Appendix C – User Rights and Privileges, of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*, contains a cross-reference table of user rights and privileges to applicable ST requirements that should be used as reference when implementing a user rights policy that must address specific ST requirements.

Assigning User Rights and Privileges

User rights can be assigned through the **Local Policies** node of **Group Policy**. As the name implies, local policies pertain to a local computer. **Local Policies** can also be configured as part of an existing **Group Policy** for a site, domain, or OU. When this is done, the **Local Policies** will apply to all computer accounts within the site, domain, or organizational unit.

Local Policies applied directly to a computer through the **Local Security Policy** interface, or **Local Computer Policy** GPO, apply only to that single computer. If the computer is a member of a domain, some of the **Local Policy** settings may be overwritten by those inherited from domain-level policies.

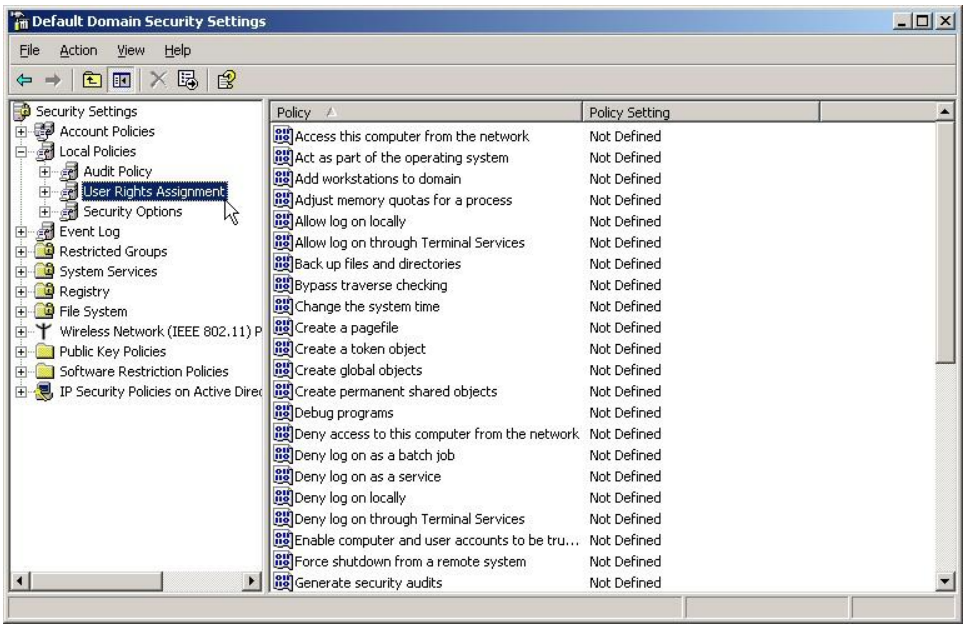
Configuring Domain-Level User Rights and Privileges

User rights policies for a domain can be administered as follows:

1. Log on using an authorized administrator for the domain.
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Local Policies** and select **User Rights Assignment**. The right-hand details pane will display the configurable logon rights and privileges.

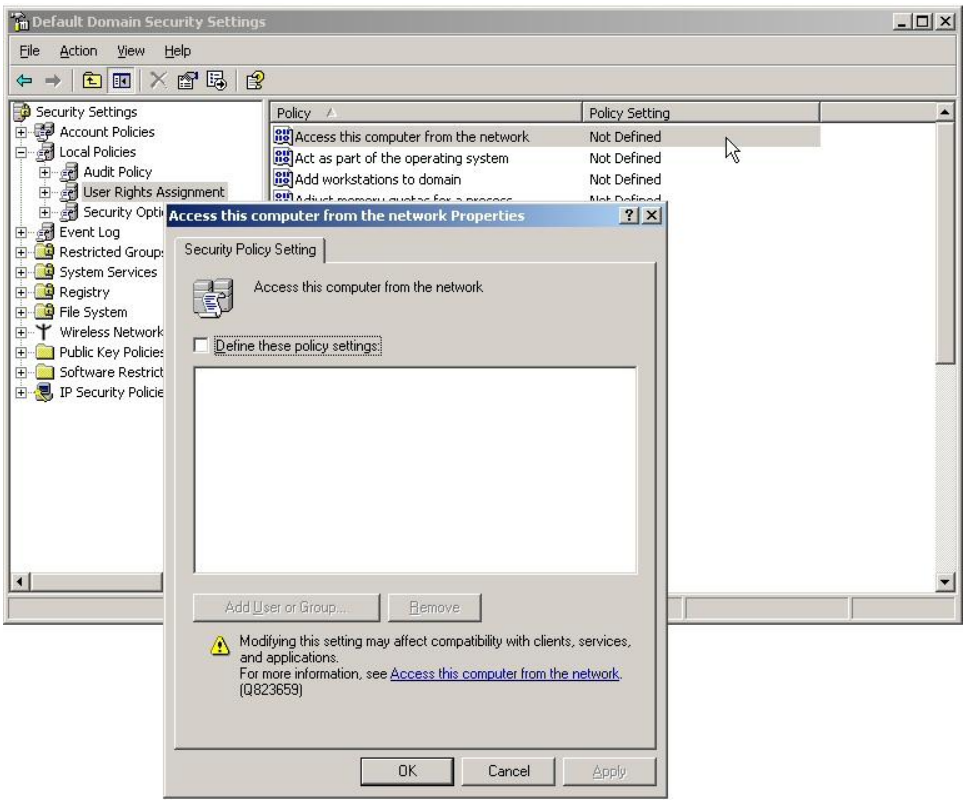
Copyright © 2008 Microsoft Corporation.

All rights reserved.



Note: All policies are either defined or not defined. That is, they are either configured for use or not configured for use. A policy that is not defined in the current GPO could be inherited from a lower level GPO.

4. To configure a **User Rights Assignment** policy, double-click a logon right or privilege, or right-click on it and select **Properties**. This opens a **Properties** interface for the logon right or privilege.



For a site, domain, or organizational unit, individual user rights can be configured by completing the following steps:

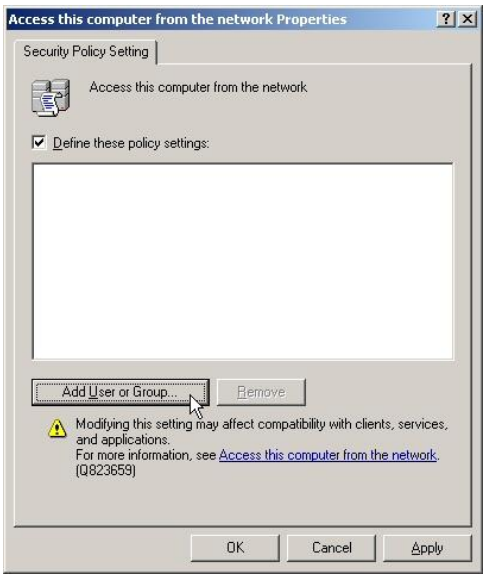
Copyright © 2008 Microsoft Corporation.

All rights reserved.

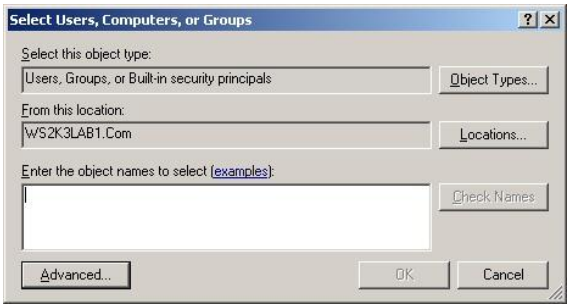
1. Open the **Properties** interface for the logon right or privilege to be modified.

   Note: For a site or OU, open the appropriate GPO and access the user right as described above in the **Domain Security Policy** procedures.

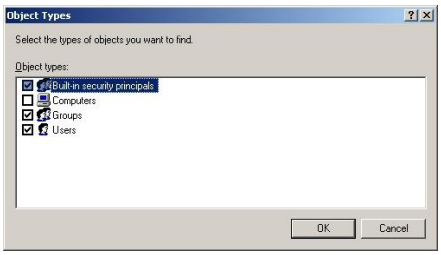
2. Select **Define these policy settings** to define the policy. To apply the right to a user or group, click the **Add User or Group** button.



3. In the **Add user or group** interface, click **Browse**. This opens the **Select Users, Computers, or Groups** interface. The logon right or privilege can now be applied to users and groups. The following selection options appear on the **Select Users, Computers, or Groups** interface:



- **Object Types:** Determines the types of objects that will be searched when trying to find or verify an account.



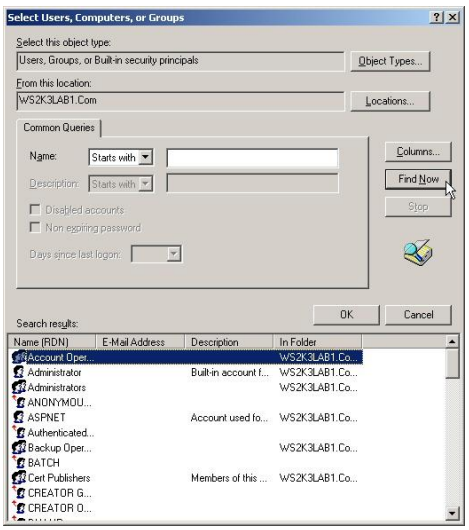
- **Locations:** To access account names from other domains, click the **Locations** button. A **Locations** interface will appear that shows the current domain, trusted domains, and other

Copyright © 2008 Microsoft Corporation.
All rights reserved.

resources that can be accessed. Select **Entire Directory** to view all the account names in the directory.

Note: Only domains that have been designated as trusted are available in the **Locations** interface. Because of the transitive trusts in Windows Server 2003, this usually means that all domains in the domain tree or forest are listed. A transitive trust is one that is not established explicitly. Rather, the trust is established automatically based on the forest structure and permissions set in the forest.

- **Advanced:** As seen in previous examples, clicking the **Advanced** button opens a **Select Users, Computers, or Groups** search tool that can be used to find accounts in the specified location.



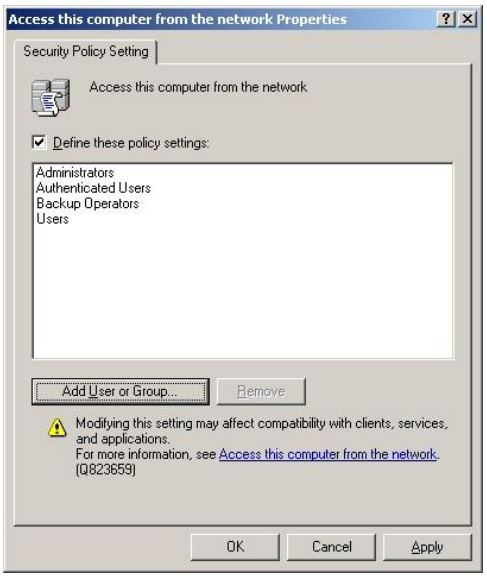
- **Check Names:** Validate the user and group names entered into the selection list. This is useful if names are typed in manually and it is necessary ensure that they're actually available.

4. After selecting the account names to add to the group, click **OK**. The **Add user or group** interface should now show the selected accounts. Click **OK** again.

5. The **Security Policy Setting** interface is updated to reflect the selections. If a mistake is made, select a name and remove it by clicking **Remove**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



6. When finished granting the right to users and groups, click **OK**.

Note: Some logon right or privilege changes may have an impact on the compatibility between clients, services, and applications. Attempting to make changes to these user rights will result in a confirmation notice such as the one shown below:

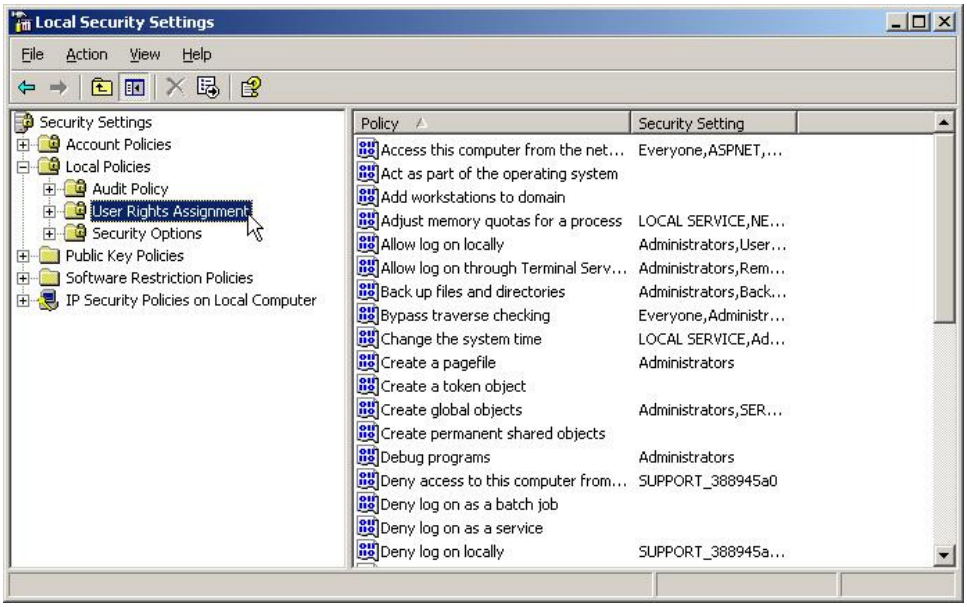
Review the information provided by the notice and proceed as necessary.

Configuring Local User Rights and Privileges

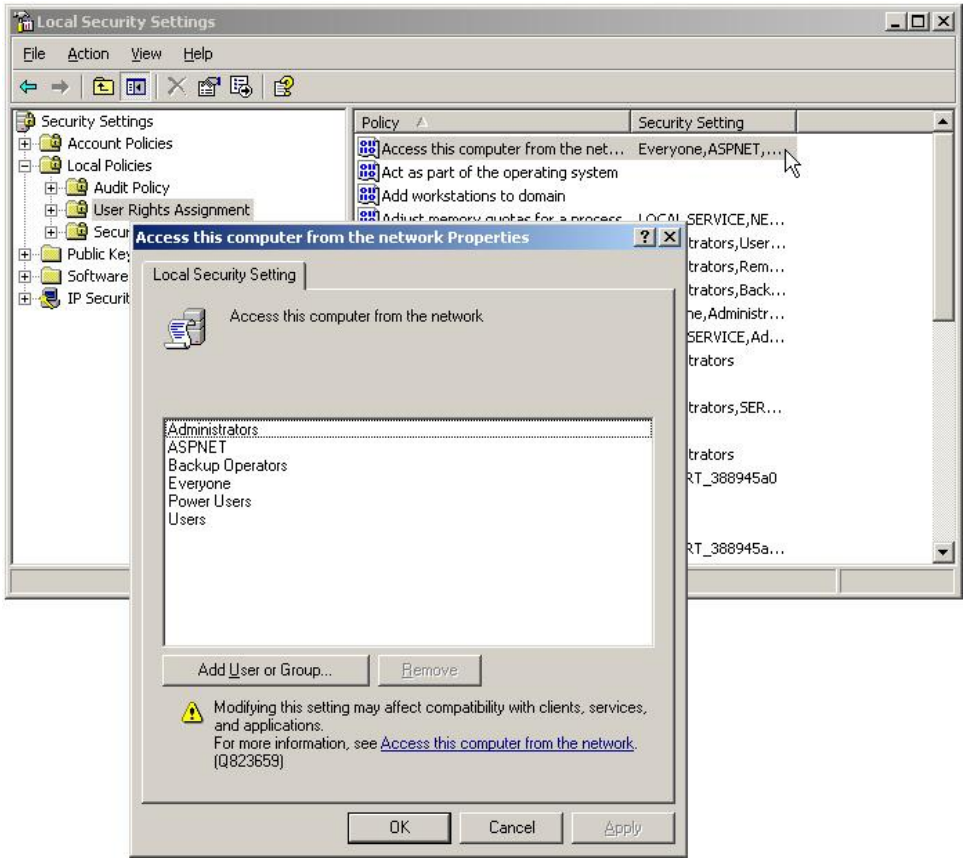
To modify user rights locally on a Windows Server 2003 computer, use the **Local Security Policy** as follows:

1. Log in as an authorized local administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Local Security Policy** from the menu. The **Local Security Settings** interface will appear.
3. Under Security Settings, expand Local Policies.
4. Select **User Rights Assignment**, to see a list of logon rights and privileges in the right-hand details pane.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. To configure user rights assignment, double-click a logon right or privilege, or right-click on it and select **Properties**. This opens a **Properties** interface for the logon right or privilege.



6. Follow the same procedures described above, in Configuring Domain-Level User Rights and Privileges, to add or remove a user or group to a logon right or privilege.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Configuring Security Options

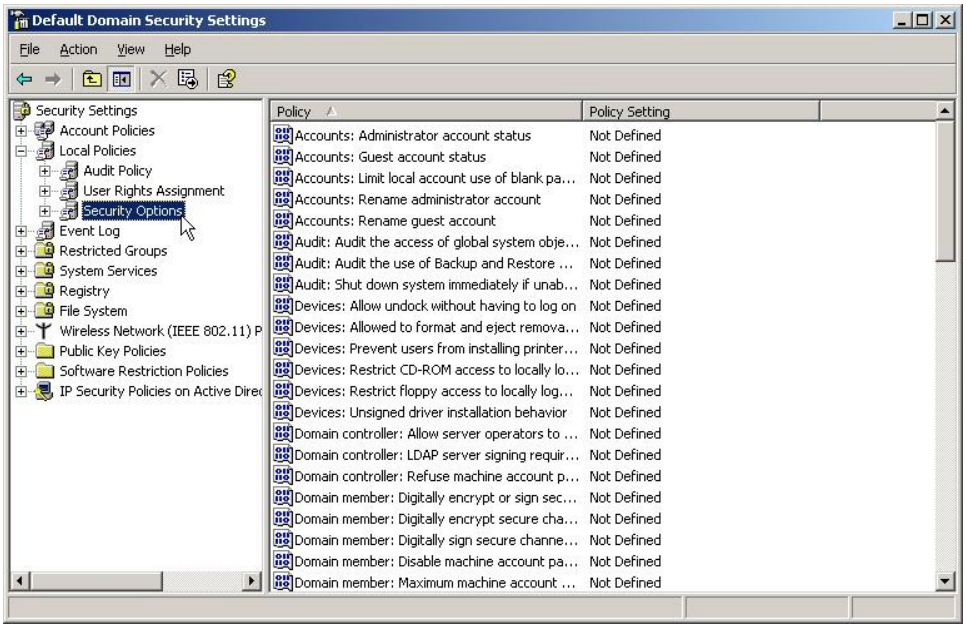
Local Policies also allow the administrator to configure **Security Options** that consist of well-known security relevant system parameters, many of which are normally configured by setting registry values using tools like **Regedit.exe**. A list of all available security relevant system parameters that can be modified through **Security Options** is provided in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*, Table 4.6, Security Option Settings. The "Required" column indicates if a security option must be enabled or disabled to meet the Windows 2003/XP V3 ST. If this column is empty then the security option may be disabled or enabled, as necessary, in the Evaluation Configuration.

Security Options are configured as follows:

1. Log on as an authorized administrator.

   Note: The example that follows illustrates use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

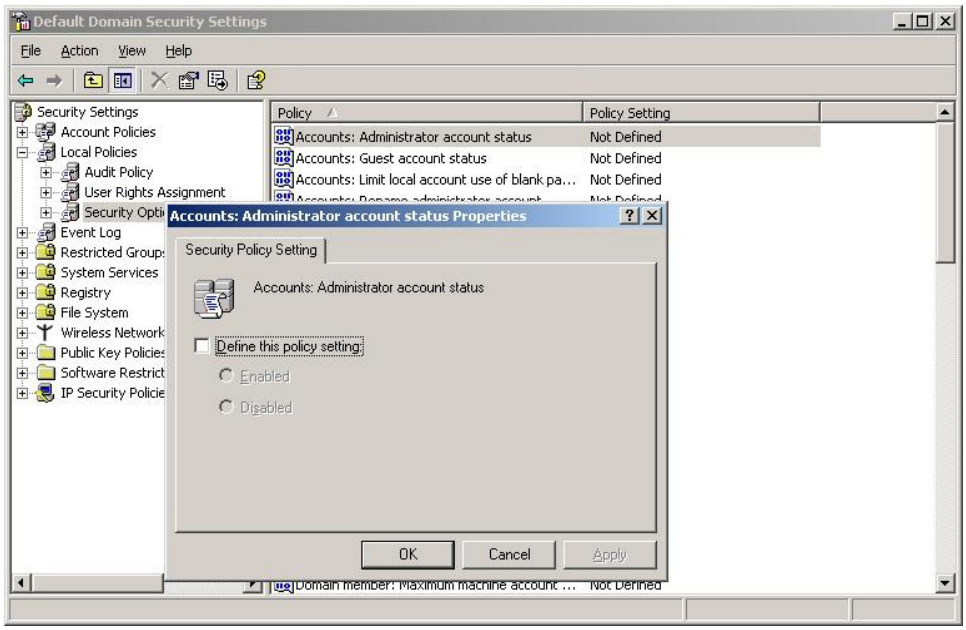
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Local Policies** and select **Security Options**. The right-hand details pane will display the configurable security settings.



4. To configure a **Security Options** policy, double-click a policy option or right-click on it and select **Properties**. This opens a **Properties** interface for the security option.

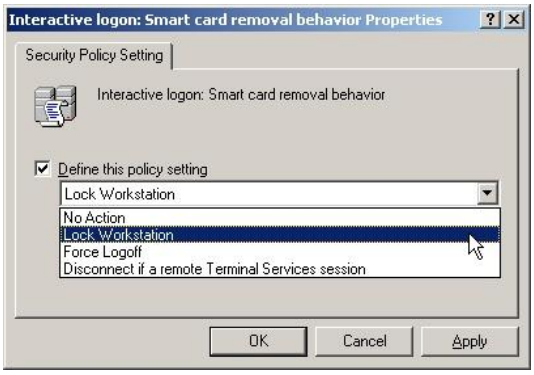
Copyright © 2008 Microsoft Corporation.

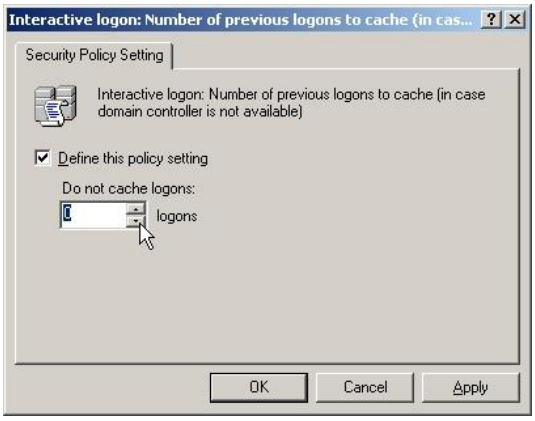
All rights reserved.



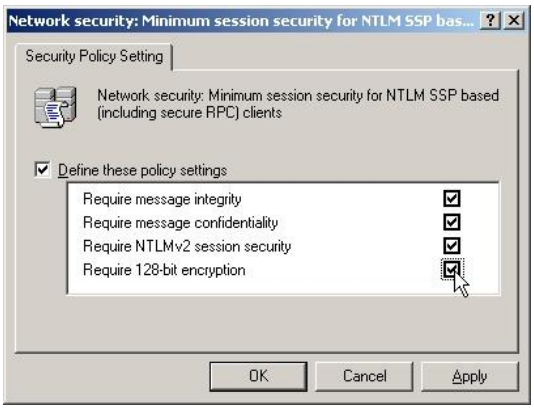
5. For domain-level policies, select **Define these policy settings** to define the policy.
6. Select to the appropriate radio button to either enable or disable the security option.
7. Click **OK** to configure the selected option.

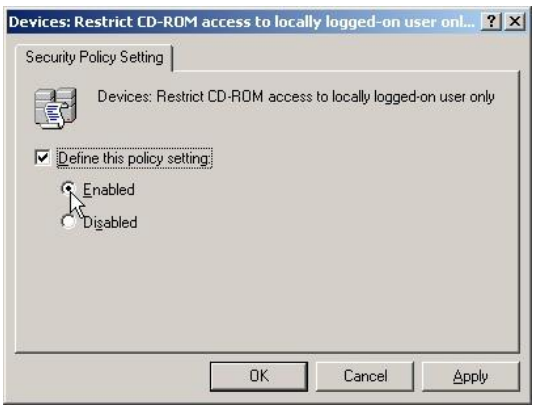
Input to the **Properties** interfaces for selected security options will vary depending on the configuration requirements of the option. For example some security options may require selection from a drop down menu, a text input, checkbox selections, or selection of an **Enabled** or **Disabled** radio button as shown below.





Copyright © 2008 Microsoft Corporation.
All rights reserved.





The subparagraphs that follow provide examples that demonstrate the implementation of ST requirements through configuration of Windows Server 2003 **Security Options** via two methods. The first method involves editing a local or domain-level security policy or a group policy. The second method involves directly editing the registry on an individual machine.

Configuring ST Requirements through the Group Policies Security Options Interface

Prevent Users from Installing Print Drivers

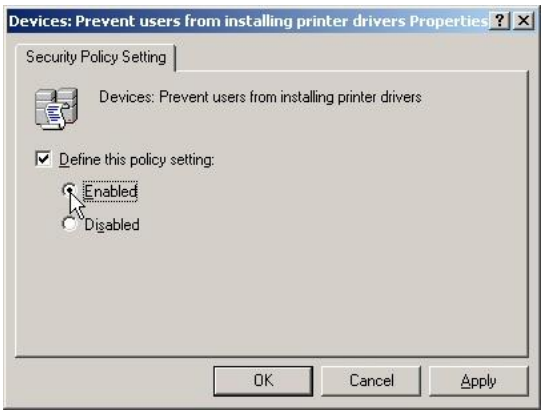
For a computer to print to a network printer, the driver for that network printer must be installed on the local computer. The **Devices: Prevent users from installing print drivers** security option setting determines who is allowed to install a printer driver as part of adding a network printer. If this setting is enabled, only members of the Administrators and Power Users groups can install a printer driver as part of adding a network printer. If this setting is disabled, any user can install a printer driver as part of adding a network printer. This setting is required for the Evaluated Configuration in order to prevent unprivileged users from downloading and installing untrusted printer drivers. Enable the **Devices: Prevent users from installing print drivers** security option as follows:

1. Log on as an authorized administrator.

   Note: The example that follows illustrates use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the Default Domain Security Settings interface.
3. Under **Security Settings**, expand **Local Policies**.
4. Select **Security Options**, to see a list of security option policies in the right-hand details pane.
5. In the details pane, double-click **Devices: Prevent users from installing print drivers**.
6. For domain-level policies, check the **Define these policy settings** check box.
7. Select the **Enabled** radio button and click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



8. Exit the Default Domain Security Settings interface.

Implementing an Authorized Usage Warning

For the Windows Server 2003 Evaluated Configuration, it is required that the system display a warning message to users before allowing them to log on. It may be necessary to get help with the wording of the message from the company's legal department. The message should inform users that the system is for authorized use only, and that they could be prosecuted if they misuse the system. For example:

> This computer system, including all related equipment, networks and network devices, are provided for the authorized use of Company XYZ employees. Use of this system constitutes consent to monitoring. Company XYZ reserves the right to monitor computer systems to ensure proper and authorized use, and to ensure that security mechanisms are not circumvented. Evidence of unauthorized use collected during monitoring may be used for administrative or legal action. Unauthorized use may be subject to criminal prosecution.

Add the logon message above to a security policy as follows:

1. Log on as an authorized administrator.

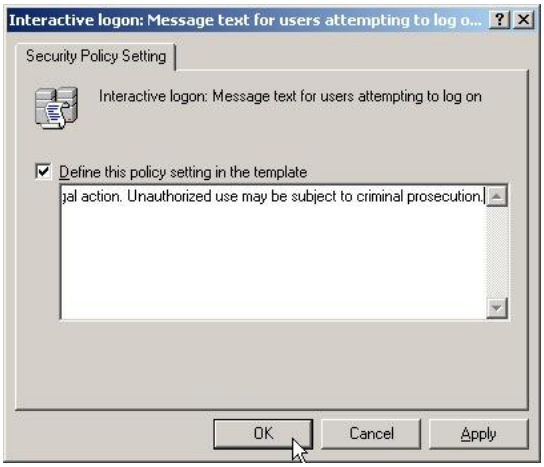
Note: The example that follows illustrates use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

---

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Under **Security Settings**, expand **Local Policies**.
4. Select **Security Options**, to see a list of security option policies in the right-hand details pane.
5. In the details pane, double-click **Interactive Logons: Message title for users attempting to log on**.
6. For domain-level policies, check the **Define this policy setting** box.
7. Enter the title for the message (for example, "Warning") and click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

8. Double-click **Interactive Logons: Message text for users attempting to log on**.
9. For domain-level policies, check the **Define this policy setting in the template** box.
10. Enter the text for the message and click **OK**.



11. Exit the Default Domain Security Settings interface.
12. Restart a domain client and log in to the domain to see the login banner message.

Since this security setting is associated with the default domain GPO, it applies to all computers in the domain. This setting will override any local policies (defined on individual computers) that specify this security parameter, but will not override any OU policies that specify this value.

Disable Shut Down Without Logging On

This security option determines whether a computer can be shut down without having to log on to Windows. When this policy is **enabled**, the **Shut Down** command is available on the Windows logon screen. When this policy is **disabled**, the option to shut down the computer does not appear on the Windows logon screen. In this case, users must be able to log on to the computer successfully and have the **Shut down the system** user right in order to perform a system shutdown. By default, this option is enabled on Windows XP Professional and disabled on Windows Server 2003.

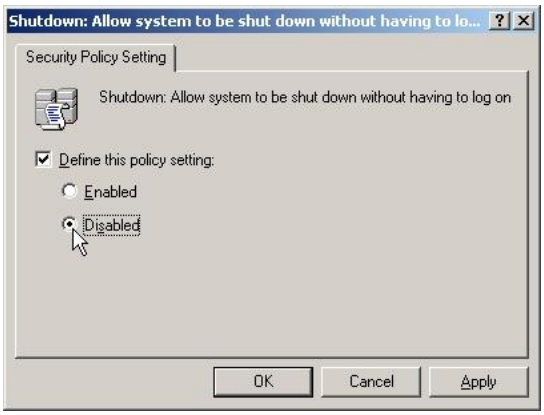
Disable the shutdown button on the Windows logon screen of Domain Computers as follows:

1. Log on as an authorized administrator.

> **Note:** The example that follows illustrates use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Under **Security Settings**, expand **Local Policies**.
4. Select **Security Options**, to see a list of security option policies in the right-hand details pane.
5. In the details pane, double-click **Shutdown: Allow system to be shut down without having to log on.**
6. For domain-level policies, check the **Define this policy setting** box.
7. Select **Disabled** and click **OK**.



8. Exit the Default Domain Security Settings interface.

Set Minimum Session Security for NTLM Security Support Provider (SSP) Based (including secure RPC) Clients and Servers

Two security options, **Network security: minimum session security for NTLM SSP based (including secure RPC) clients** and **Network security: minimum session security for NTLM SSP based (including secure RPC) servers**, are used to allow a client or a server respectively, to require the negotiation of message confidentiality (encryption), message integrity, 128-bit encryption, or NTLMv2 session security. These values are dependent on the **LAN Manager Authentication Level** security setting value. The selectable options included in this policy setting are:

- **Require message integrity:** The connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with by attaching a cryptographic signature which identifies the sender and is a numeric representation of the contents of the message. This signature ensures that the message has not been tampered with.
- **Require message confidentiality:** The connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable by anyone until decrypted.
- **Require NTLMv2 session security:** The connection will fail if the NTLMv2 protocol is not negotiated.
- **Require 128-bit encryption:** The connection will fail if strong encryption (128-bit) is not negotiated.

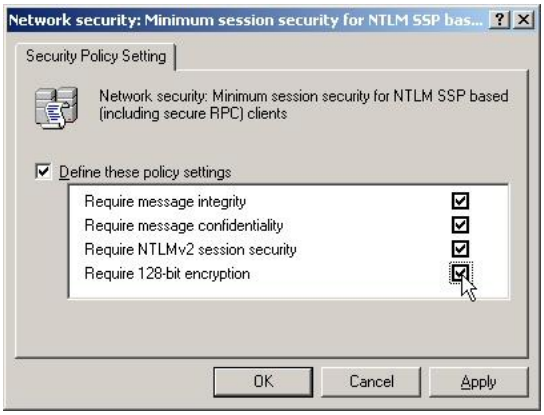
Set the minimum session security for NTLM SSP based clients and servers for the Evaluated Configuration as follows:

1. Log on as an authorized administrator.

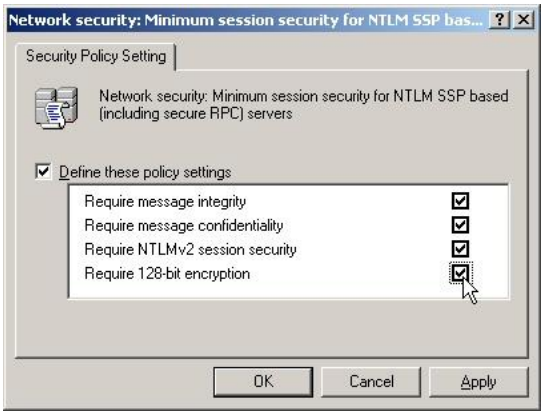
Copyright © 2008 Microsoft Corporation.
All rights reserved.

Note: The example that follows illustrates use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the Default Domain Security Settings interface.
3. Under **Security Settings**, expand **Local Policies**.
4. Select **Security Options**, to see a list of security option policies in the right-hand details pane.
5. In the details pane, double-click **Network security: minimum session security for NTLM SSP based (including secure RPC) clients**.
6. For domain-level policies, check the **Define this policy setting** box.
7. Select all of the options by checking the selection box for each of the options presented and click the **OK** button.



8. In the details pane, double-click **Network security: minimum session security for NTLM SSP based (including secure RPC) servers**.
9. Select all of the options by checking the selection box for each of the options presented and click the **OK** button.



10. Exit the Default Domain Security Settings interface.

Shut Down System Immediately If Unable to Log Security Audits

The Security Option **Audit: Shut Down System Immediately If Unable to Log Security Audits** determines whether the system should shut down if it is unable to log security events. This policy setting modifies the **Crashonauditfail** value in the SYSTEM\CurrentControlSet\Control\Lsa registry key. If this

Copyright © 2008 Microsoft Corporation.

All rights reserved.

policy is enabled, it causes the system to halt if a security audit cannot be logged for any reason. Typically, an event will fail to be logged when the security audit log is full and the retention method specified for the security log is either **Do Not Overwrite Events** or **Overwrite Events by Days**. When this security option is enabled the computer will halt and reboot, to prevent a user from taking any further action that may be auditable, if the security log becomes full and an existing entry cannot be overwritten.

By default, this policy is disabled with a registry value of zero (0). Setting the registry value to a one (1) will cause the system to halt and restart when the audit log becomes full and the value in the registry will be reset to two (2). When the system is rebooted, only an administrator account will be able to log on. The administrator will then have to archive and clear the log, reset the Registry value to one (1), and reboot the system before any other user is allowed to log on.

Note: The ST requires the system to be able to prevent auditable events from occurring, except those taken by the administrator, if the audit log becomes full. If the administrator desires this functionality, this option must be enabled. This setting should only be enabled where there is a strict audit management process in place for reviewing, archiving, and clearing the audit logs on a regular basis.

Warning: The administrative burden of enabling this setting can be very high, especially if the **Retention method for security log** is configured to **Do not overwrite events (clear log manually)**. This setting turns a repudiation threat (a backup operator could deny that they backed up or restored data) into a Denial of Service (DoS) vulnerability because a server could be forced to shut down by overwhelming it with logon events and other security events that are written to the security log. Additionally, since the shut down is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. While NTFS will guarantee that the file system's integrity will be maintained during an ungraceful system shutdown, it cannot guarantee that every data file for every application will still be in a usable form when the system restarts.

Enable this security option as follows:

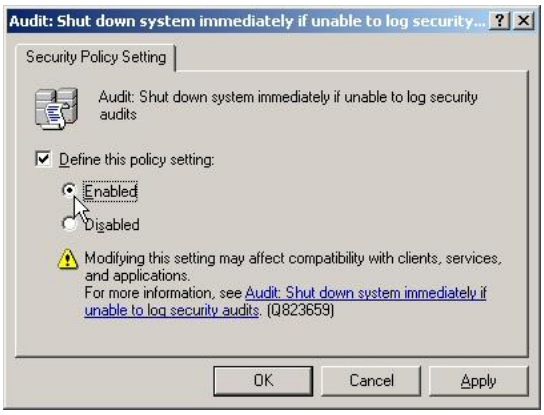
1. Log on as an authorized administrator.

   Note: The example that follows illustrates use of the **Domain Security Policy**. Procedures are similar when using a **Local Security Policy** or other domain-level policy interfaces.

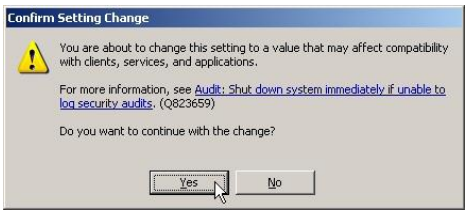
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the Default Domain Security Settings interface.
3. Under **Security Settings**, expand **Local Policies**.
4. Select **Security Options**, to see a list of security option policies in the right-hand details pane.
5. In the details pane, double-click **Audit: Shut down system immediately if unable to log security audits**.
6. For domain-level policies, check the **Define this policy setting** box.
7. Select **Enabled** and click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



8. A confirmation message will appear indicating that the change may impact compatibility between clients, servers, and applications. Review the information provided. If there is no problem for operations in the current environment, click **Yes** to apply the change.



9. Exit the Default Domain Security Settings interface.

If the audit log gets full and the system halts as a result of this setting, recover using the Registry Editor as follows:

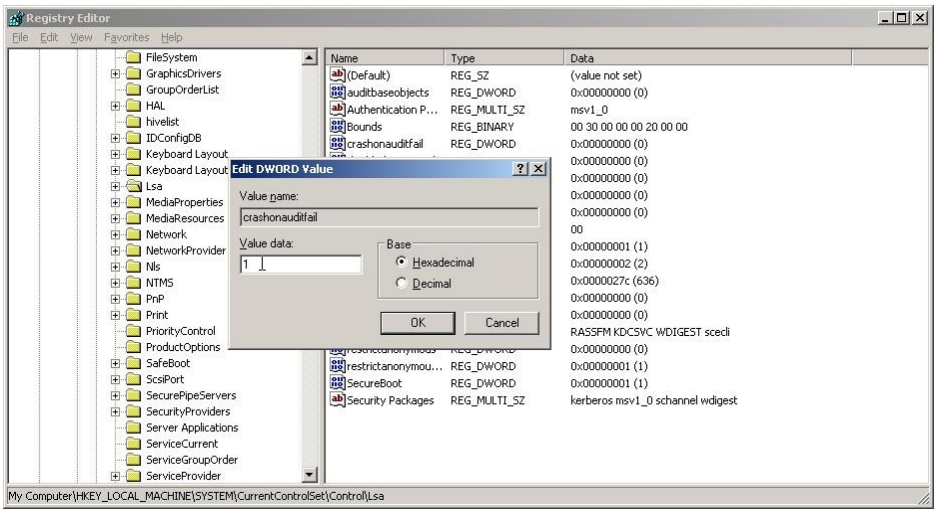
Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

---

1. Log in as an authorized administrator.
2. Archive and clear the audit log.
3. Open **Start**, select **Run**, type **regedit** and click **OK**.
4. Under the **HKEY_LOCAL_MACHINE** on Local Machine, navigate to SYSTEM\CurrentControlSet\Control\Lsa.
5. In the topic pane, double-click on **crashonauditfail**.
6. Reset the value from a 2 to a 1in the **Edit DWORD Value** window and click the **OK** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



7. Close the Registry Editor and restart the computer.

Configuring Security Target Requirements through the Registry Editor

This subsection provides one example of how the security parameters discussed above can be configured by directly editing the Windows Server 2003 Registry with the Registry Editor.

> **Warning:** Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Generate an Audit Event when the Audit Log Reaches a Percent Full Threshold

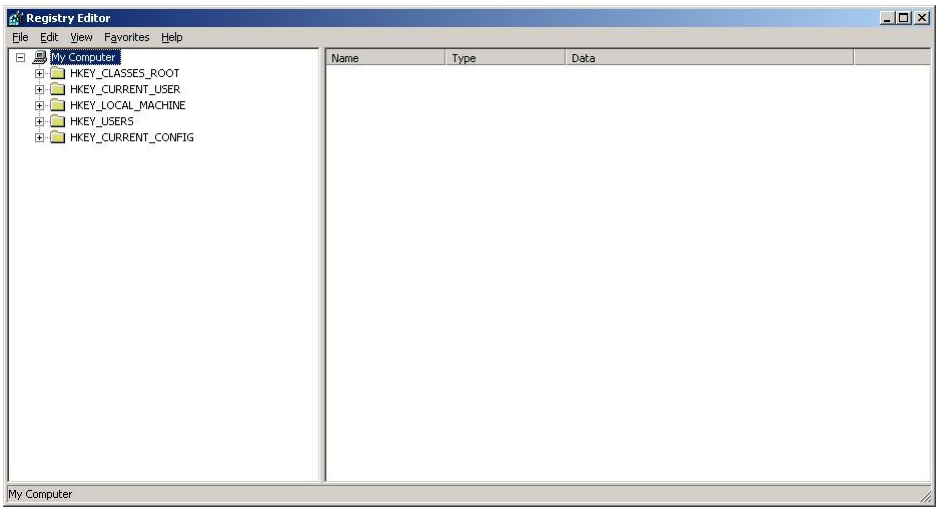
Windows Server 2003 supports a feature for generating a security audit in the security event log when the security log reaches a configurable threshold. To enable this capability, create the key value called **WarningLevel** a value setting that will designate the percent value that will cause the event to be recorded in the security log. The value can be configured to an appropriate value based on local operational needs. For example, if the value is set to **90**, and the security log size reaches the 90 percent of the preset log size, the security log will show one event entry for **eventID 523** with the following text: **The security event log is 90 percent full**. **Use extreme caution when editing the registry, because changes happen immediately and there is no option to discard changes when the Registry Editor is exited**.

> **Note:** This setting will not work if the log retention method is set to **Overwrite events as needed**.

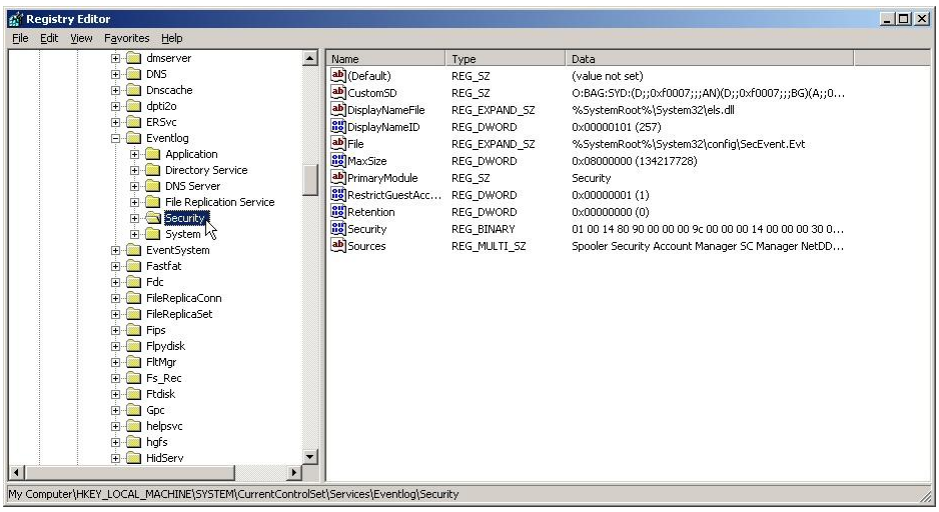
Set the audit warning level in the Registry as follows:

1. Log in as an authorized administrator.
2. To start the Registry Editor (regedit.exe) open **Start**, select **Run**, type **regedit** and click **OK**.

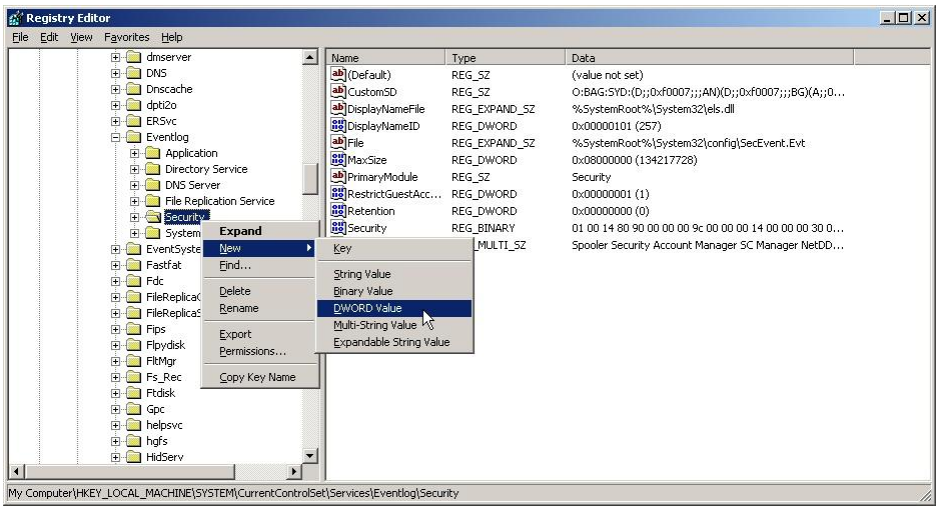
Copyright © 2008 Microsoft Corporation.
All rights reserved.



3. Under the **HKEY_LOCAL_MACHINE**, navigate to SYSTEM\CurrentControlSet\Services\Eventlog\Security.



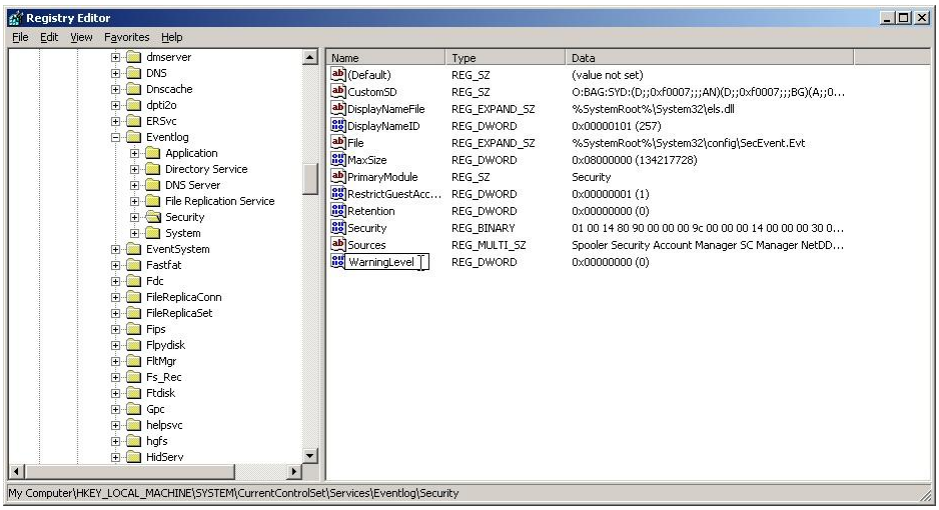
4. Right-click **Security**, point to **New**, and select **DWORD Value**.



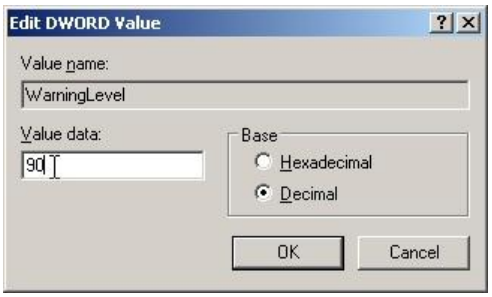
Copyright © 2008 Microsoft Corporation.

All rights reserved.

5. A new DWORD value entry will appear in the right-hand pane titled **New Value #1** by default. Rename the value to **WarningLevel**.



6. Double-click on the **WarningLevel** value to open the **Edit DWORD Value** window. Under **Base**, select the **Decimal** radio button. Under **Value data**, enter **90**. Click **OK**.



7. Close the Registry Editor and restart the computer.

RSoP Snapin

The **RSoP** snap-in enables authorized administrators to poll and evaluate the cumulative effect that local, site, domain, and OU GPOs have on computers and users. The **RSoP** snap-in enables authorized administrators to check for GPOs that might affect troubleshooting. For example, a GPO setting can cause startup programs to run after a user logs on to a computer.

Use this snap-in to evaluate the effects of existing GPOs on a computer. This information is helpful for diagnosing deployment or security problems. The **RSoP** snap-in reports individual Group Policy settings specific to one or more users and computers, including advertised and assigned applications.

Resultant Set of Policy Snap-in Core Scenarios

There are two core scenarios for the RSoP snap-in: reporting the effect of policy on various combinations of users and computers, and predicting the affect of policy. The reporting functionality of RSoP snap-in is known as **logging mode**. The predictive functionality is known as **planning mode**.

Whether in logging or planning mode, an administrator typically accesses the RSoP snap-in by opening an empty Microsoft Management Console (MMC), adding the RSoP snap-in to the console, and then using

Copyright © 2008 Microsoft Corporation.

All rights reserved.

the Resultant Set of Policy Wizard to collect data from various computers on the network for either logging or planning mode.

Logging Mode

An administrator uses logging mode to report on the current state of Group Policy settings. The scope of reports can include Group Policy settings for various targets, including a computer, a user, or both. The administrator selects combinations of targets in the Resultant Set of Policy Wizard.

When the administrator finishes with the wizard, the RSoP snap-in queries the Windows Management Instrumentation (WMI) repository on the client computer for information about the Group Policy settings for the targets. RSoP snap-in displays these settings.

Logging mode in the RSoP snap-in is useful for troubleshooting Group Policy. The RSoP snap-in lists each policy setting, and from which GPO the displayed setting came. GPO precedence is also available, as is any error information that was logged by either the Group Policy engine or any of the Group Policy client side extensions. Using this information, an administrator can determine which GPOs are applying a Group Policy setting and which GPOs are not.

In addition to using an empty MMC to access RSoP snap-in, there is another scenario an administrator is just as likely to use for troubleshooting Group Policy settings. An administrator can run RSOP.msc from the command prompt on a client computer to report on the current computer with the current user logged on. In this manner, the administrator avoids having to select targets in the Resultant Set of Policy Wizard.

Planning Mode

An administrator uses planning mode to perform "what if" scenarios with Group Policy. Like logging mode, the end result is a report of Group Policy settings. However, unlike logging mode, this report contains simulated data.

The administrator uses RSoP snap-in and a Windows Server 2003 Domain Controller. First, the administrator must use the Resultant Set of Policy Wizard to define the scope of the report. This is done by selecting various targets. In planning mode these targets must include both user information and computer information; however, the administrator can select either a particular user or computer or an Active Directory container for users or computers.

After specifying the scope of the plan, the administrator uses the wizard to specify a simulated Group Policy settings environment. Because these Group Policy environment settings are simulated, an actual client computer might behave differently in live tests. It is not possible for a domain controller to accurately determine how a particular client computer will actually behave.

The following simulated environment settings are available:

- A slow network connection
- Loop-back processing (merge mode and replace mode)
- Site-based policy implementation
- Security group memberships for the user, the computer, or both
- WMI Filters that are linked to the user, the computer, or both

The administrator can elect to simulate any, all, or none of the environment variables. Whatever the choices, when the wizard finishes, the RSoP snap-in requests a simulation of policy from the domain controller. The domain controller uses Resultant Set of Policy Provider to simulate the application of GPOs. This service passes the GPO settings to virtual client-side extensions on the domain controller. The results of the simulation are stored in the WMI repository on the domain controller before the information is passed back to the RSoP snap-in for analysis. It is important to remember that the results

Copyright © 2008 Microsoft Corporation.

All rights reserved.

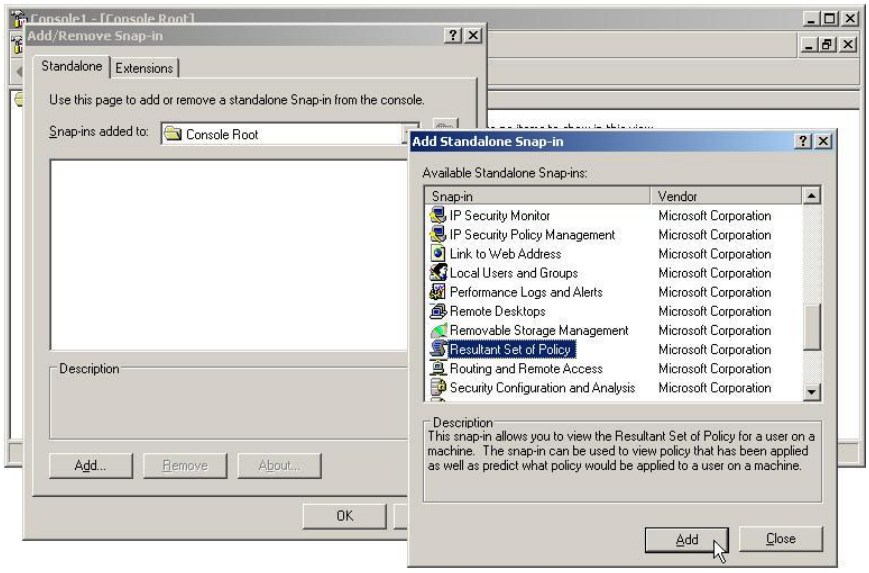
displayed in the RSoP snap-in are not actual Group Policy settings, but simulated Group Policy based on the settings created using the wizard. If a custom client side extension exists on a client but does not exist on the domain controller, then any Group Policy settings this custom client side extension might create would not appear in the simulation results.

Planning mode in the RSoP snap-in is useful for planning Group Policy. The RSoP snap-in lists each GPO from which the displayed setting came as well as any other lower priority GPOs that attempted to configure settings. Using this information, an administrator can determine which GPOs are applying a policy setting and which GPOs are not.

Using the RSoP Snap-in

To use the **RSoP** snap-in:

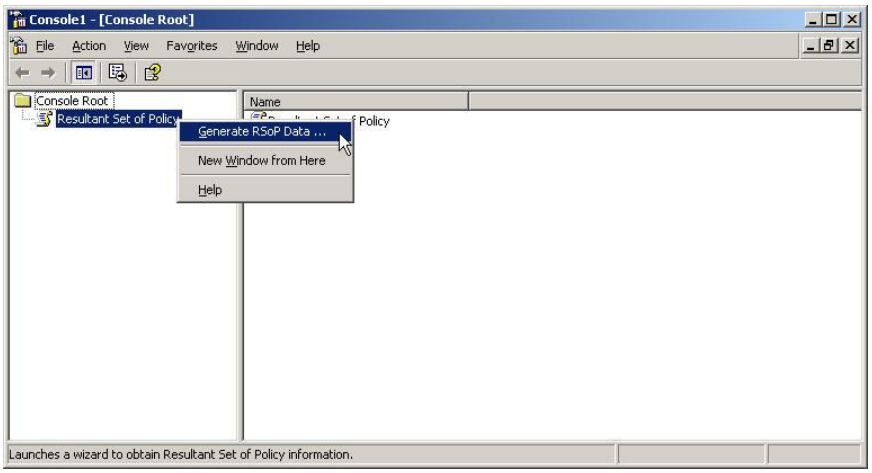
1. Log on as an authorized administrator.
2. Click on **Start** and select **Run**.
3. Type **mmc** in the **Open** box, and then click **OK**.
4. Click **File**, click **Add/Remove Snap-in**, and then click **Add** in the **Add/Remove** dialog box.
5. Select **Resultant Set of Policy**, click **Add**, and then click **Close** in the **Add/Remove Standalone Snap-in** dialog box.



6. Click **OK** in the **Add/Remove** dialog box. The **Resultant Set of Policy** snap-in is displayed in the MMC.
7. Right-click on the **Resultant Set of Policy** object in the MMC and select **Generate RSOP data**.

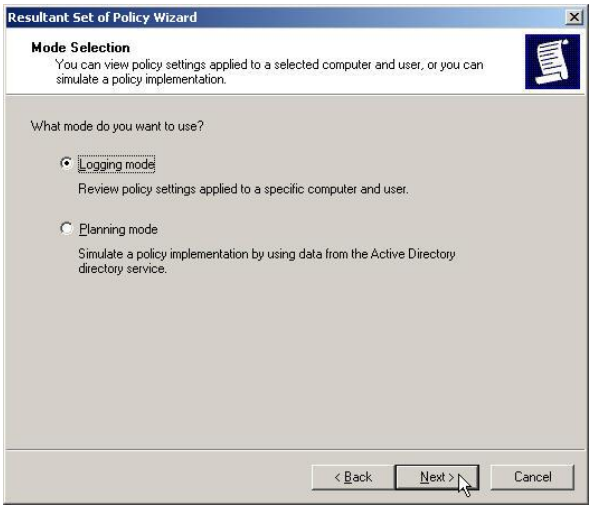
Copyright © 2008 Microsoft Corporation.

All rights reserved.



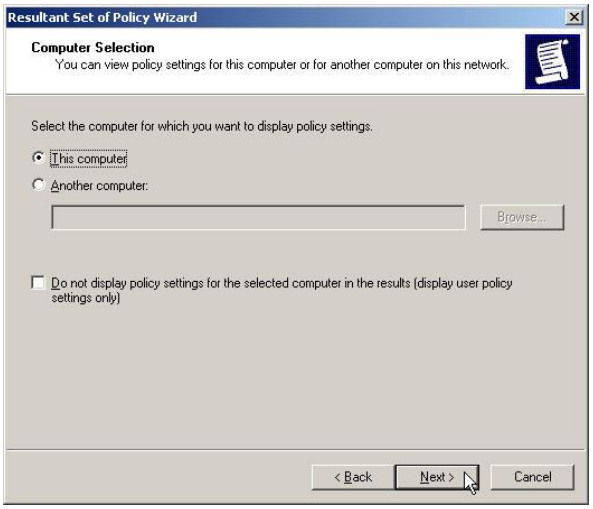
8. The Resultant Set of Policy Wizard will be displayed. Click **Next**.

9. The **Mode Selection** page of the Wizard will be displayed. Select the **Logging mode** radio button, and then click **Next**. If the computer in not in a domain, the **Planning mode** radio button will be disabled.

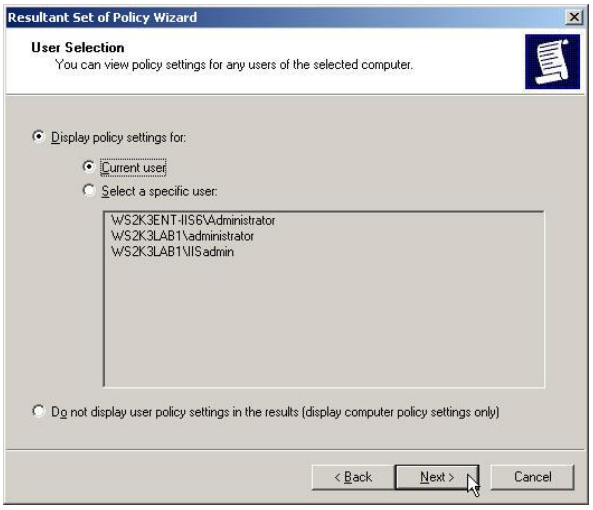


Copyright © 2008 Microsoft Corporation.
All rights reserved.

10. The **Mode Selection** page of the Wizard will be displayed. If the **Another computer** radio button is selected, the **Browse** button may be used to find the remote computer on the network. A check box can be selected so that only user settings are presented in the results and computer settings are not shown. For this example, select the **This computer** radio button and do not select the check box. Click **Next**.



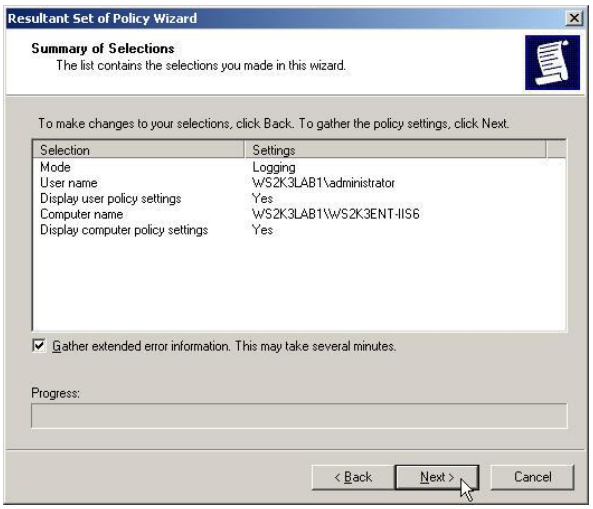
11. The **User Selection** page of the Wizard will be displayed. Select the **Display policy settings for** radio button and the **Current user** radio button, then click **Next**.



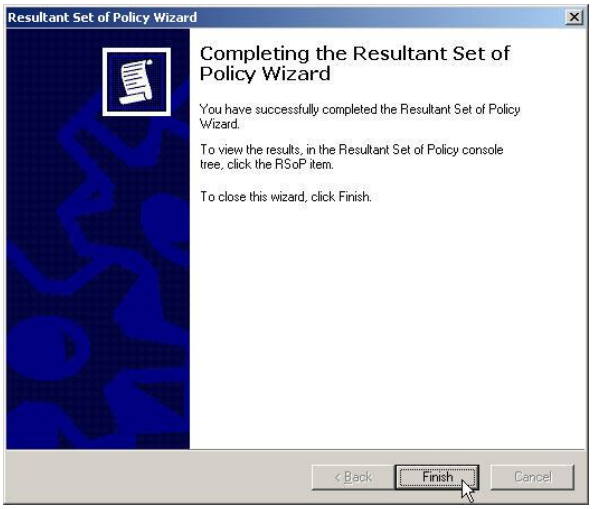
12. The **Summary of Selections** page of the Wizard will be displayed. Review the information in the summary. If changes are required, click the **Back** button to find the location where the changes are required and make the necessary edits. When finished, click **Next**.

Copyright © 2008 Microsoft Corporation.

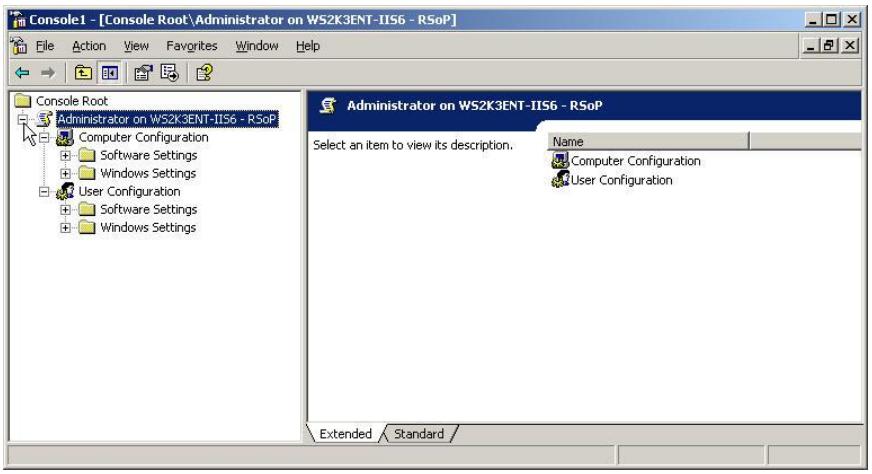
All rights reserved.



13. The Wizard will display the progress of the RSoP in gathering policy settings. When this task completes, the **Completing the Resultant Set of Policy Wizard** page will be displayed. Click **Finish** to complete the Wizard.

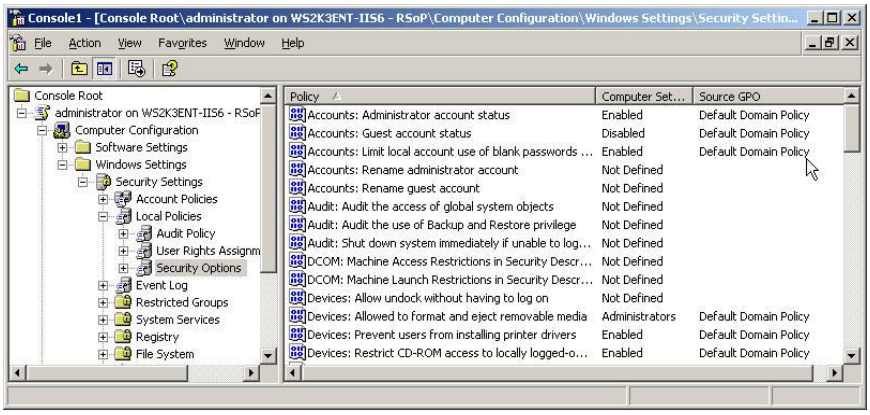


14. To view the collected policy categories, expand the **RSoP node** in the MMC.



15. Navigate through the RSoP results to view the various group policy settings and their source GPOs.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



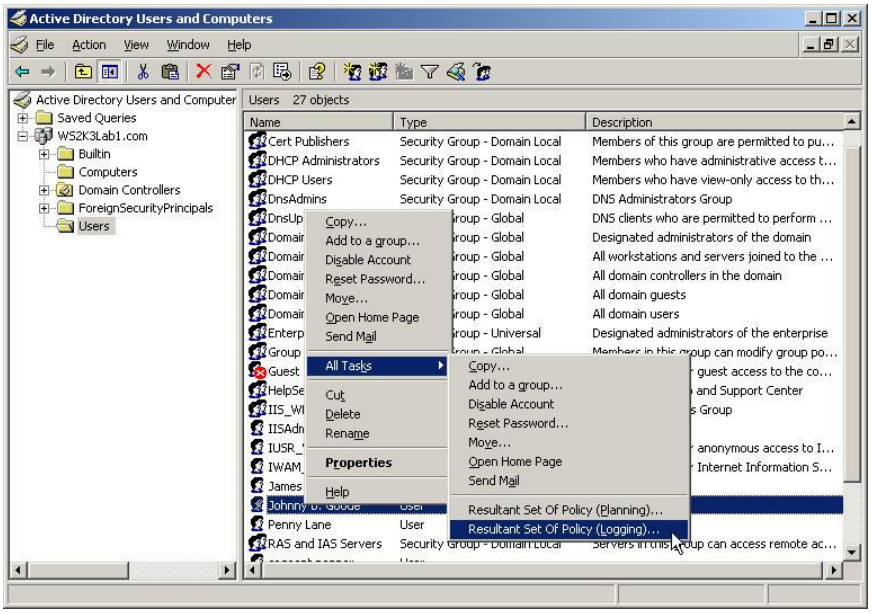
Using the RSoP from a Domain Controller

On a Domain Controller, a domain administrator can execute the RSoP from within the Active Directory Users and Computers interface to conduct an RSoP query of a computer account, user account, domain, or OU. The Active Directory Sites and Services interface can be used to conduct an RSoP query of a specific Active Directory site.

Note: In order to conduct an RSoP query of a domain user on a client computer, the user must have logged into the client computer at least once.

As an example, to conduct an RSoP query of user account on domain client computer:

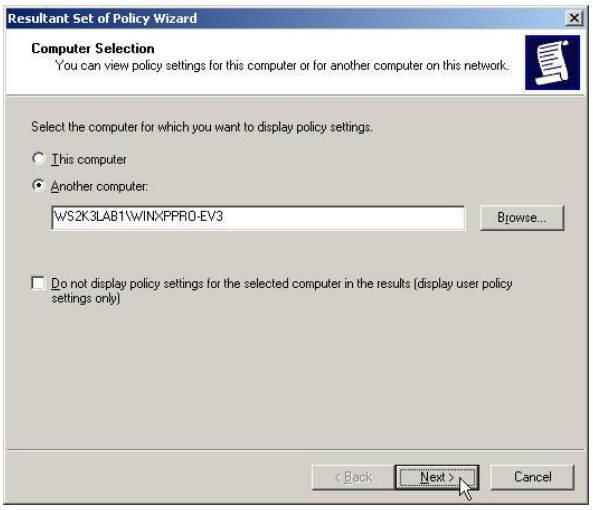
1. Log on as a domain administrator.
2. Click on **Start**, point to **Administrative Tools** and select **Active Directory Users and Computers**.
3. Expand the domain node. Then right-click on a user account, point to **All Tasks**, and select **Resultant Set Of Policy (Logging)**.



4. In the Computer Selection page of the Resultant Set of Policy Wizard, select the **Another computer** radio button. Enter the name of the client computer, or click the **Browse** button to find the computer. Click **Next**.

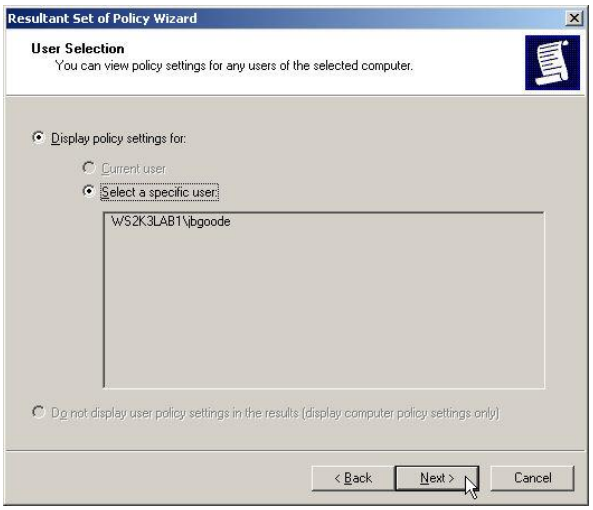
Copyright © 2008 Microsoft Corporation.

All rights reserved.



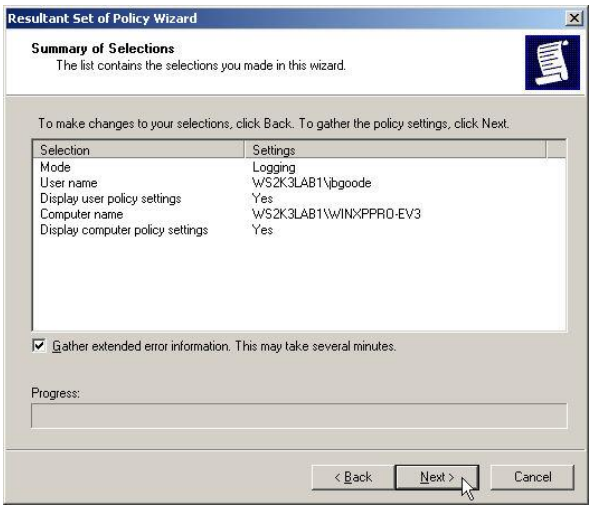
Note: If the Windows Firewall is enabled on the client with the default firewall settings, the RSoP query will fail.

5. Click **Next** on the **User Selection** page of the Wizard.

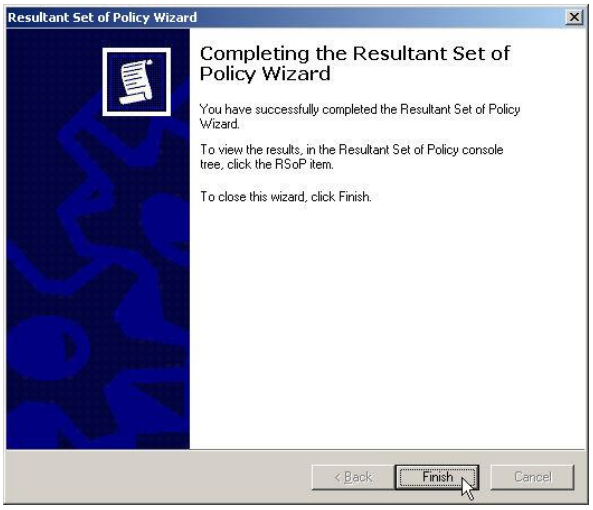


6. Review the information in the **Summary of Selections** page, and click **Next** if the information is correct. To make corrections, click the **Back** button.

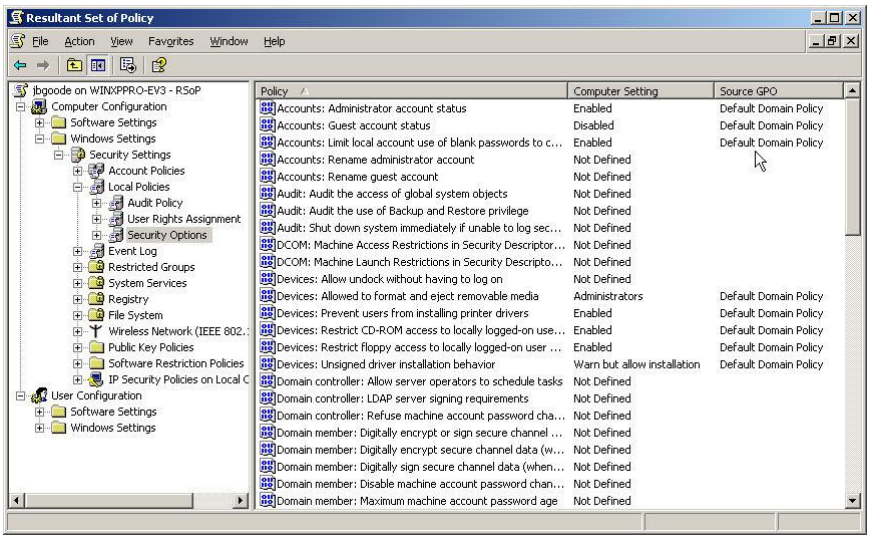
Copyright © 2008 Microsoft Corporation.
All rights reserved.



7. Click **Finish** to complete the Resultant Set of Policy Wizard.



8. The RSoP results will be displayed. Navigate through the RSoP results to view the various group policy settings and their source GPOs.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

Creating and Maintaining User and Group Accounts

A local user or group is an account that is created and can be granted permissions and rights on a local computer. Domain or global users and groups are managed by the network administrator. Local users, global users, and global groups can be added to local groups. However, local users and groups cannot be added to global groups. Global, Domain Local, and Universal groups are managed from a Domain Controller.

User and group accounts are important in Windows Server 2003 security because they are used to control the ability of users to perform certain actions by granting specific logon rights, privileges, and permissions to their user and group accounts. Logon rights are used to grant or deny a user or group of users various methods of logging on locally or remotely. Privileges authorize a user or group to perform certain actions on a computer, such as backing up files and folders or shutting down a computer. A permission is a rule associated with an object (usually a file, folder, or printer), and it regulates which users can have access to the object and in what manner.

Appendix D of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* provides a description of the user and group accounts available in Windows Server 2003 and the account requirements and recommendations for the Evaluated Configuration.

Computer Accounts

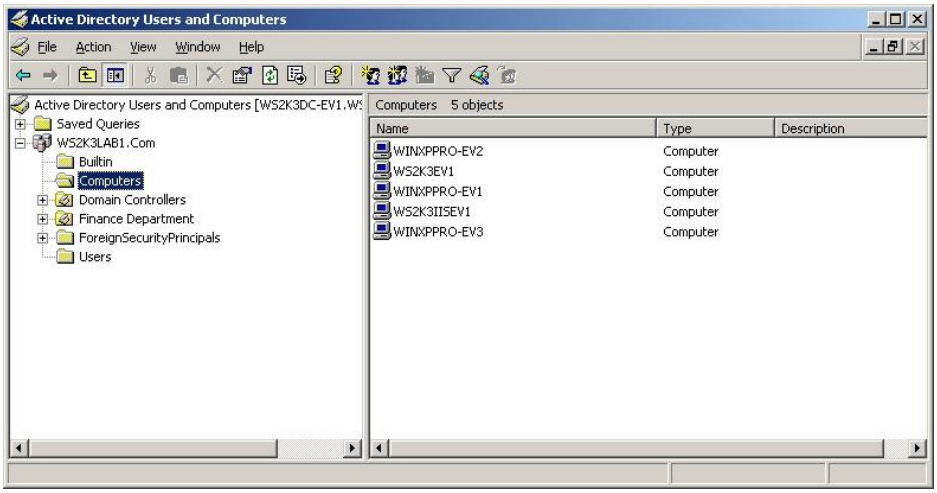
Every computer running Windows XP Professional or Windows Server 2003 that is joined to a domain by an authorized administrator is automatically assigned a computer account within the domain. Similar to user accounts, computer accounts provide a means for authenticating and auditing a computer's access to the network, and to domain resources. Each computer connected to the network must have its own unique computer account.

Computer accounts may also be created by a domain administrator using **Active Directory Users and Computers** and later joined to the domain by a user. This allows domain administrators to authorize a computer account into the domain without having to log on to the computer locally to add to the domain.

Adding and Deleting Computer Accounts

To add a computer account:

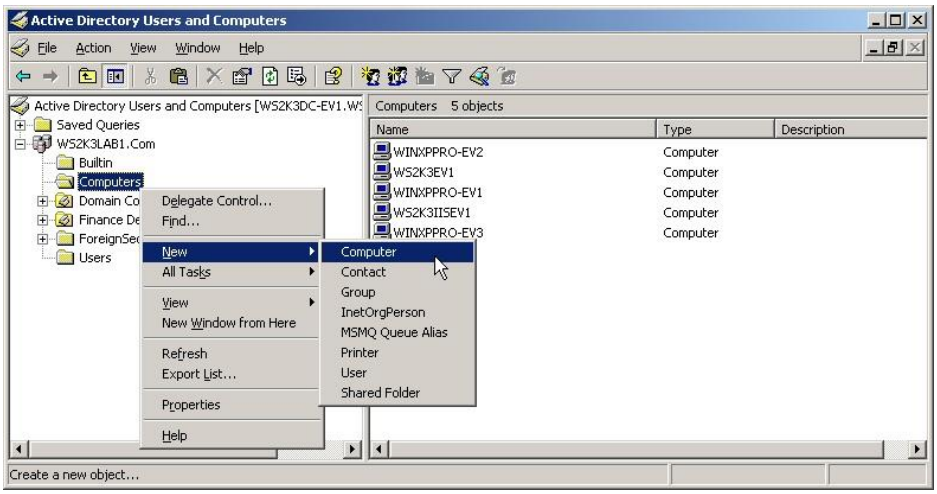
1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.



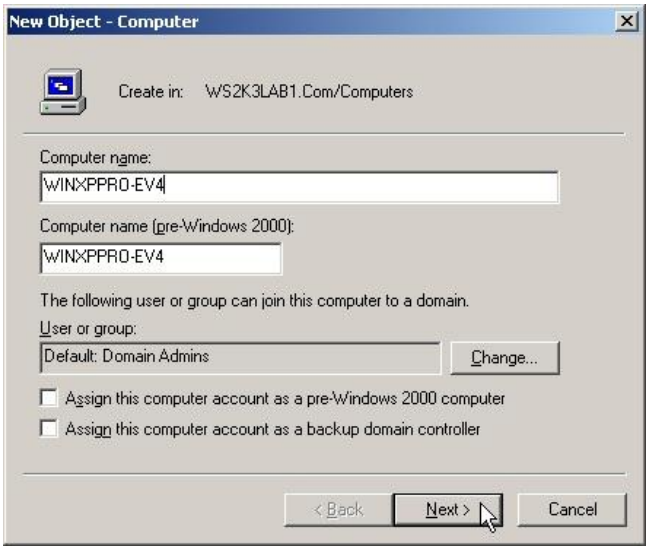
Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. In the console tree, right-click **Computers** or click the on the container in which the computer is to be added, point to **New**, and then click **Computer**. A **New Object – Computer** window will appear.



4. Enter the computer name. The **Default Domain Policy** settings enable only members of the group Domain Admins to add a computer account to a domain. Click the **Change** button to specify a different user or group that can add this computer to the domain. Click **Next**.

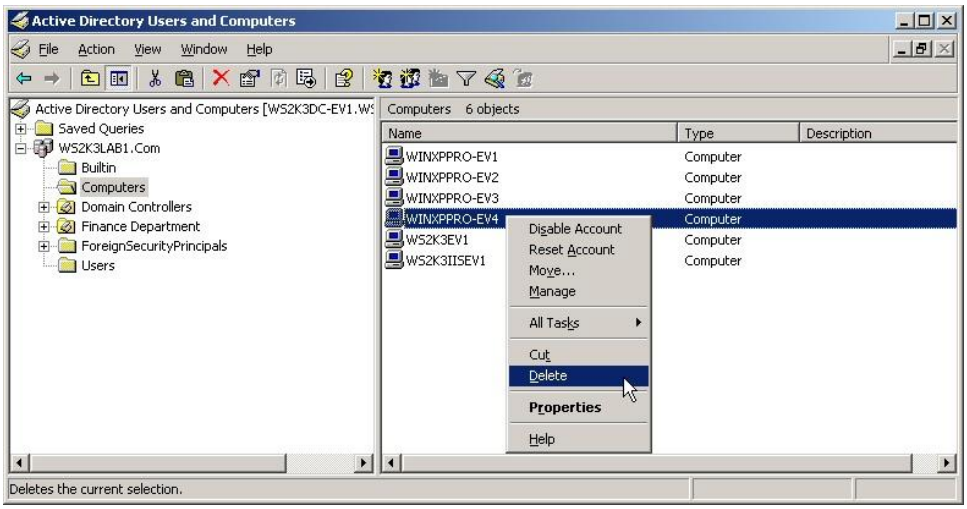


5. If this is to be a managed computer, enter the requested information. Click **Next**.
6. Click **Finish** to create the computer account.

To delete a computer account:

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
2. In the console tree, click **Computers,** or click the folder in which the computer is located.
3. In the details pane, right-click the computer, and then click **Delete**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

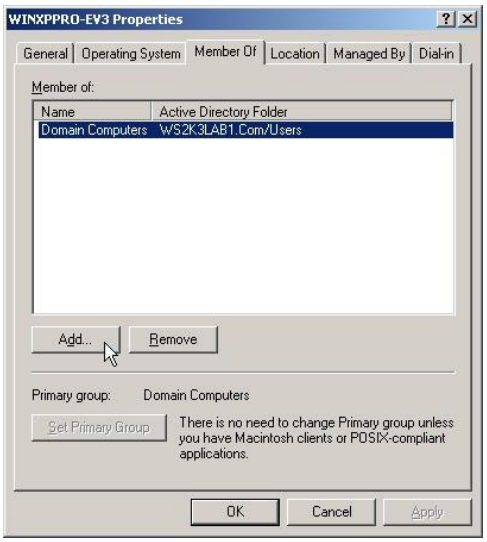


Adding a Computer Account to a Group

Adding a computer account to a group allows for the assignment of permissions to all of the computer accounts in that group and for filtering of Group Policy settings for all accounts within that group.

To add a computer account to a group:

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, click **Computers**. Or, click the folder in which the computer is located.
4. In the details pane, right-click the computer, and then click **Properties**.
5. On the **Member Of** tab, click **Add**.



6. Use the **Advanced** search feature of the **Select Groups** interface to search for the group to which the computer is to be added. By default all domain member computers are members of the **Domain Computers** group.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Group Accounts

Group accounts are used to manage logon rights and privileges for multiple users. Global group accounts, for domain use, are created in **Active Directory Users And Computers,** while local group accounts, for local system use, are created in **Local Users And Groups**. Generally, group accounts are created to facilitate the management of similar types of users. The types of groups that can be created include the following:

- **Groups for departments within the organization:** Generally, users who work in the same department need access to similar resources. Because of this, groups can be created that are organized by department, such as Business Development, Sales, Marketing, or Engineering.
- **Groups for users of specific applications:** Often, users will need access to an application and resources related to the application. Application-specific groups can be created so that users get proper access to the necessary resources and application files.
- **Groups for roles within the organization:** Groups could also be organized by the user's role within the organization. For example, executives probably need access to different resources than supervisors and general users. Thus, by creating groups based on roles within the organization, proper access is given to the users that need it.

Group Scope and Group Type

Each security and distribution group has a scope that identifies the extent to which the group is applied in the domain tree or forest. There are three different scopes: universal, global, and domain local.

- Groups with **Universal Scope** can have as their members groups and accounts from any Windows Server 2003 domain in the domain tree or forest and can be granted permissions in any domain in the domain tree or forest. Groups with **Universal Scope** are referred to as universal groups.
- Groups with **Global Scope** can have as their members groups and accounts only from the domain in which the group is defined and can be granted permissions in any domain in the forest. Groups with a **Global Scope** are referred to as global groups.
- Groups with **Domain Local Scope** can have as their members groups and accounts from a Windows Server 2003 domain and can be used to grant permissions only within a domain. Groups with a **Domain Local Scope** are referred to as domain local groups.

In the case of multiple forests, users defined in only one forest cannot be placed into groups defined in another forest, and groups defined in only one forest cannot be assigned permissions in another forest.

The following table summarizes the behaviors of the different group scopes.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Universal scope	Global scope	Domain local scope
When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of universal groups can include accounts, global groups, and universal groups from any domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of global groups can include accounts and global groups from the same domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of domain local scope can include accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain.
When the domain functional level is set to Windows 2000 mixed, security groups with universal scope cannot be created.	When the domain functional level is set to Windows 2000 mixed, members of global groups can include accounts from the same domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of domain local groups can include accounts and global groups from any domain.
When the domain functional level is set to Windows 2000 native or Windows Server 2003, groups can be added to other groups and assigned permissions in any domain.	Groups can be added to other groups and assigned permissions in any domain.	Groups can be added to other domain local groups and assigned permissions only in the same domain.
Groups can be converted to domain local scope. Groups can be converted to global scope, as long as no other universal groups exist as members.	Groups can be converted to universal scope, as long as the group is not a member of any other group with global scope.	Groups can be converted to universal scope, as long as the group does not have as its member another group with domain local scope.

Changing Group Scope

When creating a new group, by default, the new group is configured as a security group with global scope regardless of the current domain mode. Changing a group scope can be accomplished by the following allowed conversions:

- **Global to universal**. This is only allowed if the group is not a member of another group having global scope.
- **Domain local to universal**. The group being converted cannot have as its member another group having domain local scope.

Note: Changing a group scope is not allowed in mixed-mode domains. Note that mixed-mode domains are not part of the Evaluated Configuration.

Group Types

There are two types of groups in Windows Server 2003:

- **Security groups**. A group that can be listed in Discretionary Access Control Lists (DACLs) used to define permissions on resources and objects. A security group can also be used as an e-mail entity. Sending an e-mail message to the group sends the message to all the members of the group.
- **Distribution groups**. A group that is used solely for e-mail distribution and that is not security-enabled. Distribution groups cannot be listed in DACLs used to define permissions on resources and objects. Distribution groups can be used only with e-mail applications (such as Microsoft Exchange)

Copyright © 2008 Microsoft Corporation.

All rights reserved.

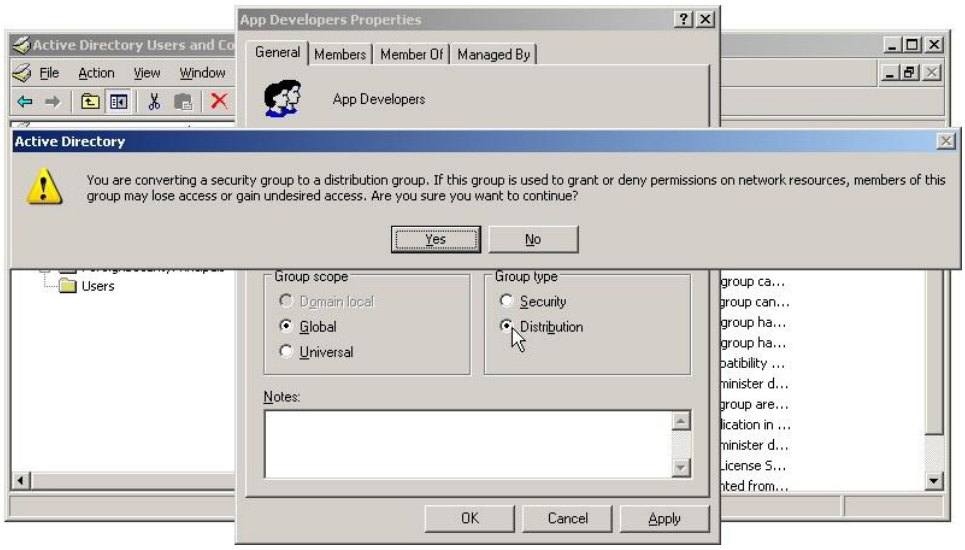
to send e-mail to collections of users. If a group is not needed for security purposes, create a distribution group instead of a security group.

Note: Although a contact can be added to a security group as well as to a distribution group, contacts cannot be assigned rights and permissions. Contacts in a group can be sent e-mail.

Converting between Security and Distribution Groups

A group can be converted from a security group to a distribution group, and vice versa, at any time, but only if the domain is in native-mode. No groups can be converted while a domain is in mixed-mode.

- When attempting to a group type from convert from a security group to a distribution group the following warning will be presented:



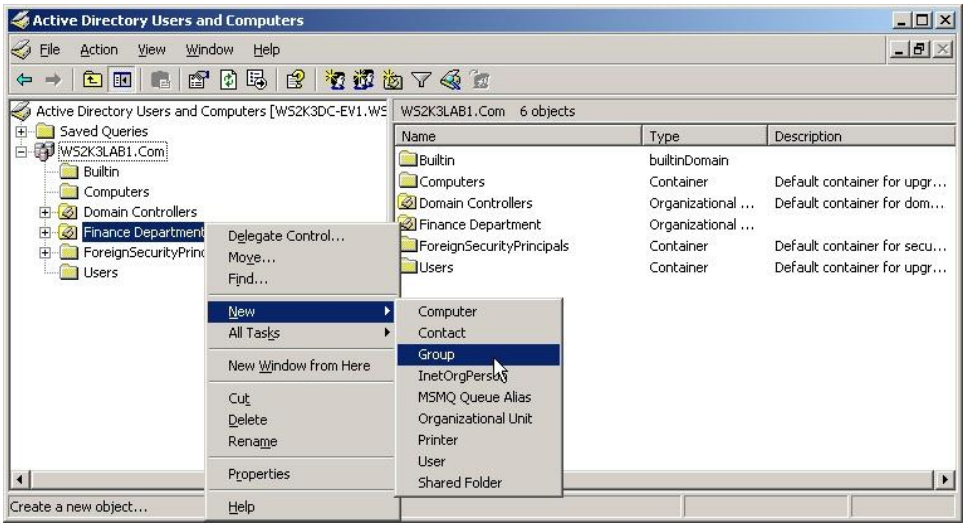
- Any attempt to change a security group that is also the primary group of a user, to a distribution group will not be allowed. The attempt will result in a warming message stating that a group with primary members cannot change to a security-disabled group.
- Conversely, care must be taken to evaluate permissions, privileges, and group memberships associated with any group that is changed from a distribution group to a security group. Any user that is originally a member of a distribution group and then gets changed to a security group would gain any new privileges and access rights associated with the newly converted security group.

Creating Group Accounts

Add a group account to the domain as follows:

1. Log on to the Domain Controller as an authorized administrator.
2. Open **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, double-click the domain node.
4. Right-click the folder in which the group is to be added, point to **New**, and then select **Group**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



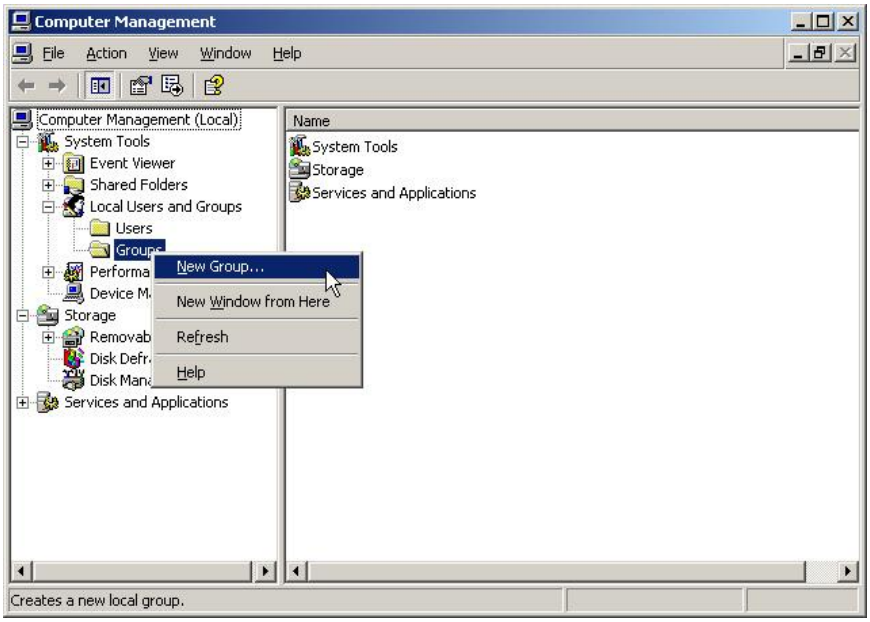
5. Type the name of the new group. By default, the name that is typed is also entered as the pre-Windows 2000 name of the new group.
6. Select the desired **Group scope**.
7. Select the desired **Group type**.

8. Click **OK**. The new group will appear in the details pane of the Active **Directory Users and Computers**.
9. Modify logon rights and privileges for the new group as explained in the Configuring User Rights subsection of this document. These procedures may be used by authorized administrators to modify user logon rights and privileges at any time by assigning or removing logon rights and privileges as required.

Add a local group account to a Windows Server 2003 server as follows:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools,** and then select **Computer Management**.
3. Expand **Local Users and Groups**.
4. Right-click the **Groups** folder and select **New Group**.

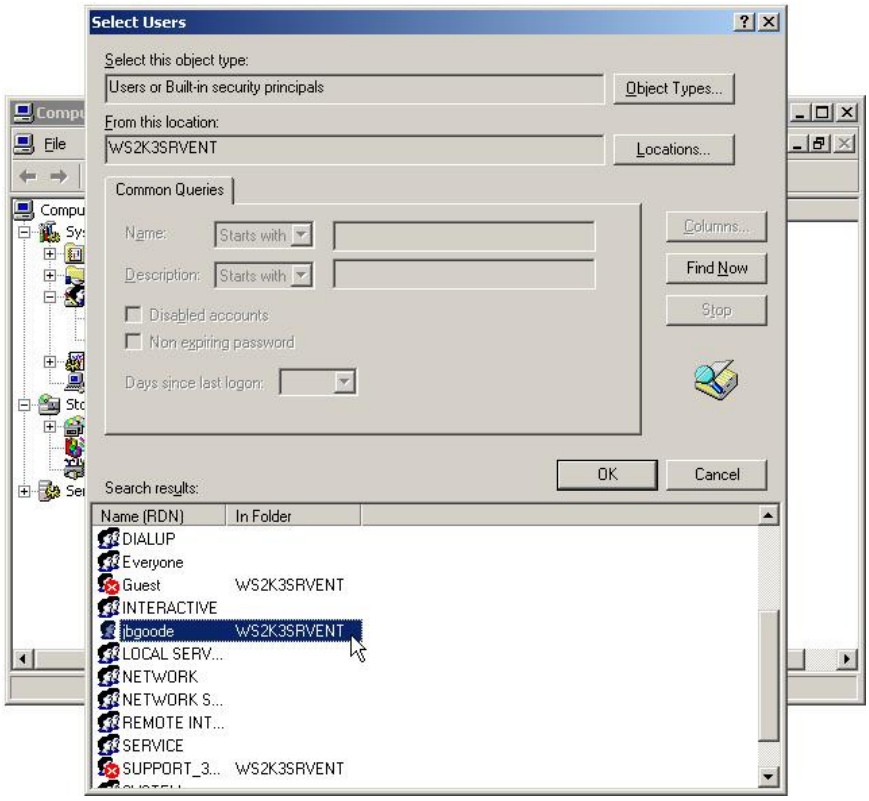
Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. Enter a group name and, if desired, a description. Click the **Add** button to add users to the group.

6. Use the **Advanced** button of the **Select Users** interface to search for user accounts.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



7. Click **OK** on the **Select Users** search tool after selecting an account. Click **OK** on the **Select Users** interface.
8. Click the **Create** button on the **New Group** interface to create the group with the selected members.

9. The **New Group** interface will clear in preparation for creating another group. If there are no other groups to create, click the **Close** button.

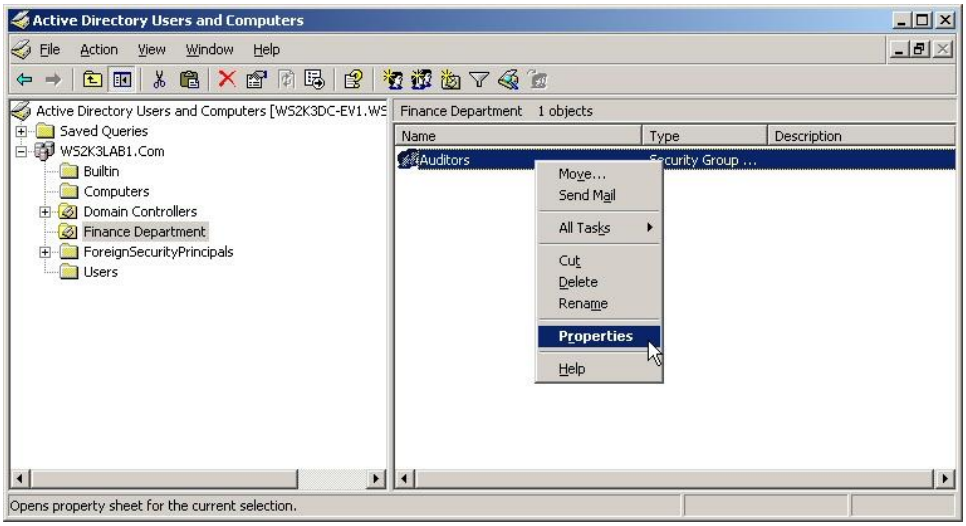
Adding Group Members

Add members to a group within a domain as follows:

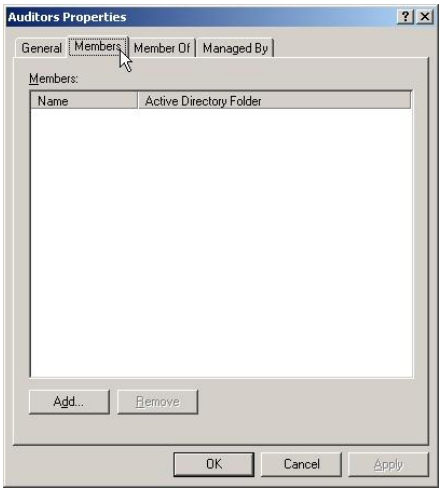
1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. In the console tree, click the folder that contains the desired group account.
4. In the details pane, double-click the desired group account, or right-click the group and select **Properties** from the menu.

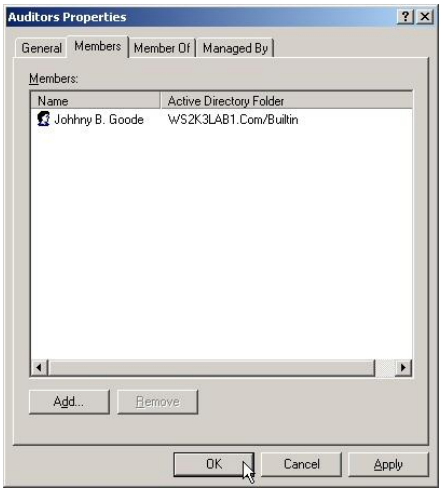


5. In the **Properties** window, click the **Members** tab.



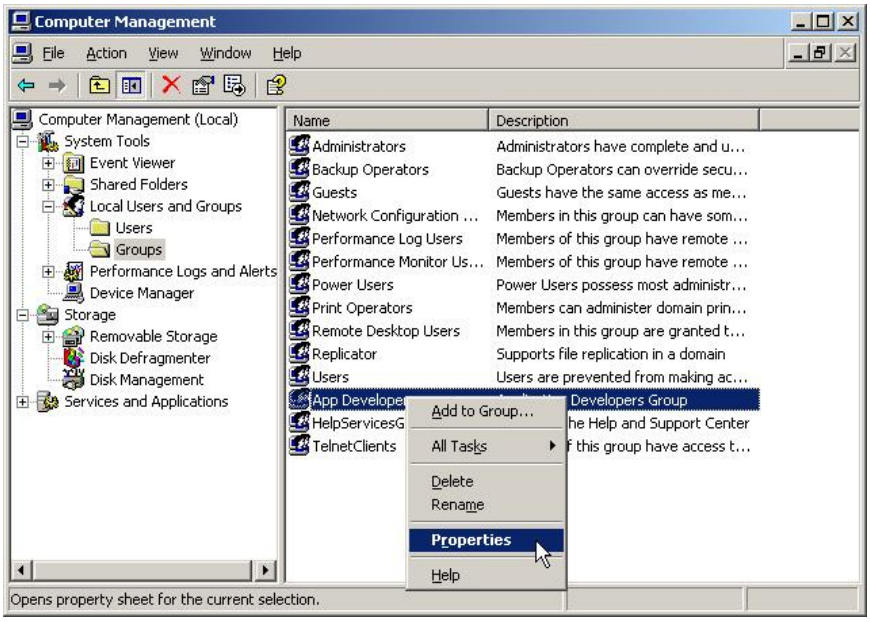
6. Click **Add**. The Select Users, Contacts, or Computers interface appears.
7. Enter user accounts or use the **Advanced** button of the Select Users, Contacts, or Computers interface to search for user accounts.
8. Click **OK** on the Select Users search tool after selecting an account. Click **OK** on the Select Users interface.
9. When there are no more users to add, click **OK** in the group Properties interface.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



Add members to a local group on a stand-alone Windows Server 2003 computer as follows:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand **Local Users and Groups** and select **Groups**.
4. Right-click the on the group to which users will be added and select **Properties**.



5. Click the **Add** button and use the **Advanced** button of the **Select Users** interface to search for user accounts.
6. Click **OK** on the **Select Users** search tool after selecting an account. Click **OK** on the **Select Users** interface.

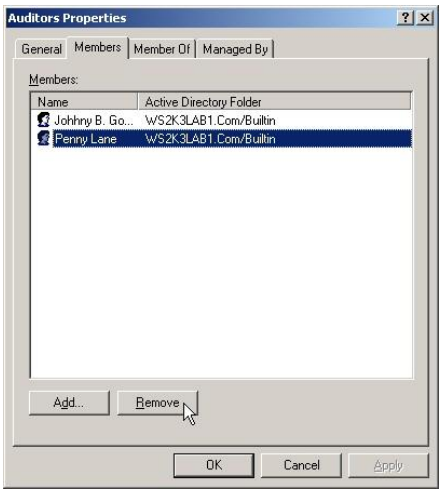
Copyright © 2008 Microsoft Corporation.
All rights reserved.

Removing Group Members

Remove members from a group as follows:

> **Note:** The procedures below are for domain-based groups. The procedures are similar when removing accounts from local groups on Windows Server 2003 stand-alone or member servers.

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, select the folder that contains the desired group account.
4. In the details pane, double-click the desired group account, or right-click the group and select **Properties** from the menu.
5. In the **Properties** interface, click the **Members** tab.
6. From the list of group members, select the member to be removed, and click the **Remove** button.



7. An **Active Directory** confirmation message will appear. Click the **Yes** button to remove the member from the group.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Note: No confirmation message will appear when removing an account from a local group on stand-alone, or member server, Windows Server 2003 computers.

8. In the **Properties** window, click **OK**.

Nesting Groups

Adding groups to other groups (nesting groups) can reduce the number of times permissions need to be assigned. Desired groups can be nested to consolidate group management by increasing the affected member accounts and to reduce replication traffic caused by replication of group membership changes. Windows Server 2003 allows for unlimited levels of nesting in Native mode. However, tracking permissions becomes more complex with multiple levels of nesting, therefore it is important to keep the levels of nesting to a minimum.

Nesting options depend on whether the domain functionality of the Windows Server 2003 domain is set to Windows 2000 native or Windows 2000 mixed. Groups in domains set to the Windows Server 2003 native functional level or distribution groups in domains set to the Windows 2000 mixed functional level can have the following members:

- Groups with universal scope can have the following members: accounts, computer accounts, other groups with universal scope, and groups with global scope from any domain.
- Groups with global scope can have the following members: accounts from the same domain and other groups with global scope from the same domain.
- Groups with domain local scope can have the following members: accounts, groups with universal scope, and groups with global scope, all from any domain. This group can also have as members other groups with domain local scope from within the same domain.

Security groups in domains set to the Windows 2000 mixed functional level are restricted to the following types of membership:

- Groups with global scope can have as their members only accounts.
- Groups with domain local scope can have as their members other groups with global scope and accounts.

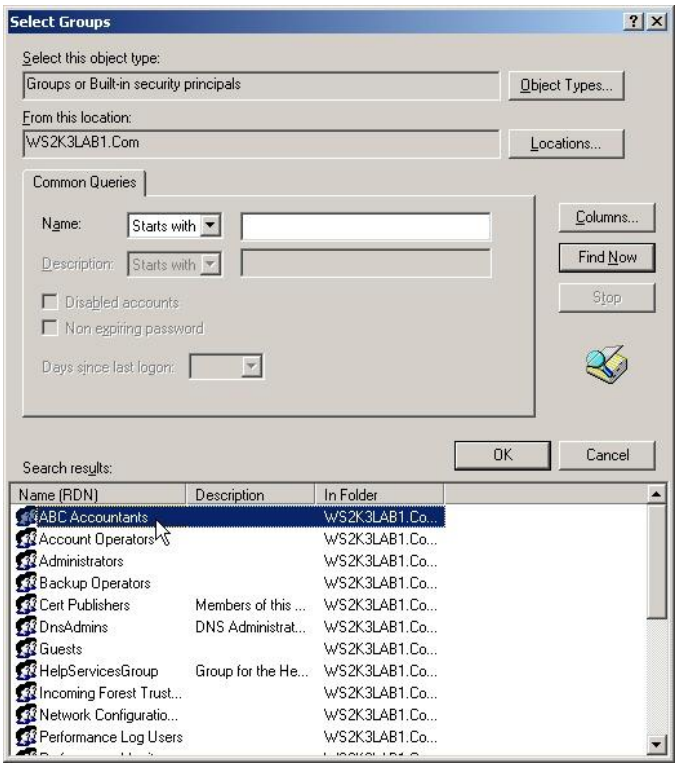
Security groups with universal scope cannot be created in domains with the domain functional level set to Windows 2000 mixed because universal scope is supported only in domains where the domain functional level is set to Windows 2000 or Windows Server 2003 native mode.

Add/modify group nesting as follows:

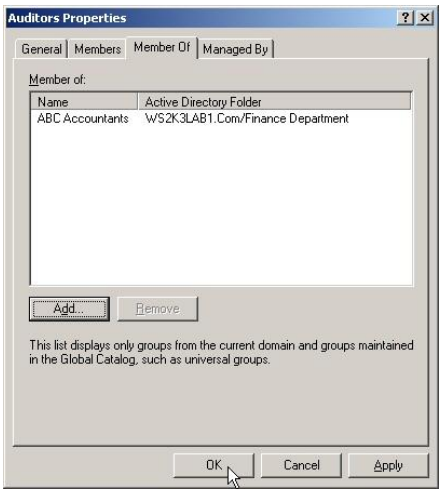
1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, click the folder that contains the desired group account.
4. In the details pane, double-click the desired group account, or right-click the group and select **Properties** from the menu.
5. In the group Properties interface, click the **Member of** tab.
6. Click **Add**. The Select Groups interface appears.
7. Use the **Advanced** button of the Select Users interface to search for groups.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



8. Click **OK** on the **Select Users** search tool after selecting a group. Click **OK** on the Select Users interface.
9. Click **OK** on the group **Properties** interface.



Deleting a Group

Warning: Each group that is created has a unique, non-reusable SID. Windows Server 2003 uses the SID to identify the group and the permissions that are assigned to it. When a group is deleted, Windows Server 2003 does not use the SID again, even if a new group is created with the same name as the group that was deleted. Therefore, simply re-creating a deleted group cannot restore access to resources.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

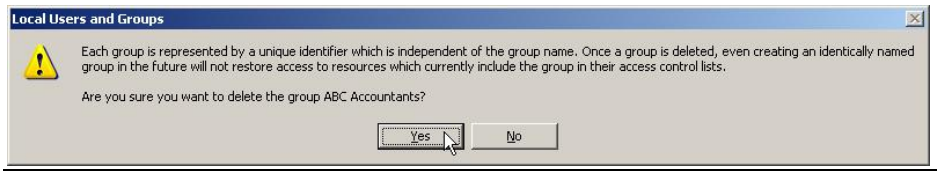
A group may be deleted as follows:

1. Log on as an authorized administrator.

Note: The procedures below are for domain-based groups. The procedures are similar when removing accounts from local groups on Windows Server 2003 stand-alone or member servers.

2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, click Groups or the folder that contains the desired group account.
4. In the details pane, right-click the group and select **Delete**.
5. An Active Directory confirmation window will appear.

Note: When deleting a group account from a stand-alone, or member server, Windows Server 2003 computer the confirmation message will appear as shown below.



6. Click **Yes** to delete the group.

User Accounts

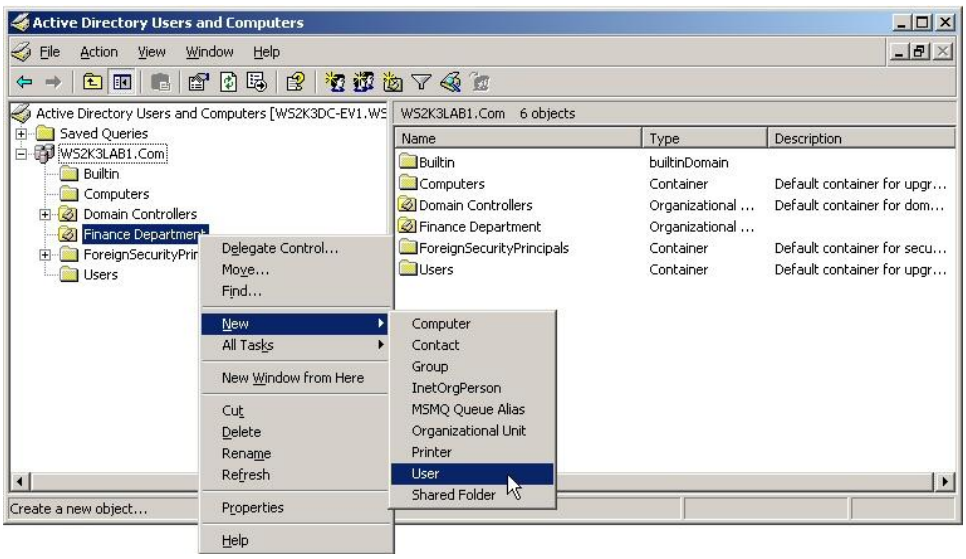
This subsection provides procedures for creating and managing user accounts.

Creating User Accounts

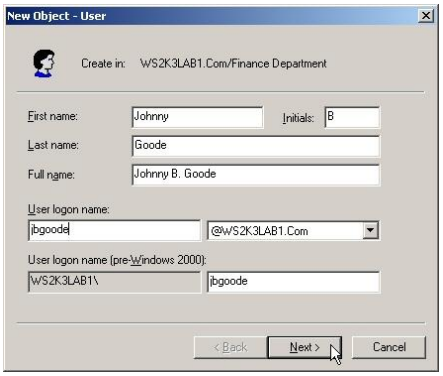
Add a user account to the domain as follows:

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, double-click the domain node.
4. Right-click the organizational unit where the user is to be added, point to **New**, and then select **User**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. Type first name, initials, and last name.
6. In **User logon name**, type the name that the user will log on with and, from the drop-down list, click the User Principal Name (UPN) suffix that must be appended to the user logon name (following the @ symbol). Click **Next**.

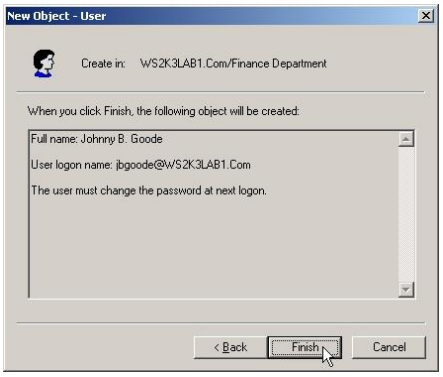


7. Enter an initial login password for the user in the **Password** text box and confirm the password by entering it again the **Confirm password** text box. For the Evaluated Configuration, passwords must be eight (8) characters in length or greater. If the password complexity requirements security policy has been implemented, the password must not contain all or part of the user's account name, and must contain characters from at least three (3) of four (4) classes; English Upper Case Letters, English Lower Case Letters, Base ten digits, and/or special characters (e.g., !,$,#,%). Make sure the **User must change password at next logon** box is checked to force users initially logging on to create a new password that is not known to administrators. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

8. Review the user object settings. If everything is correct, click **Finish**.

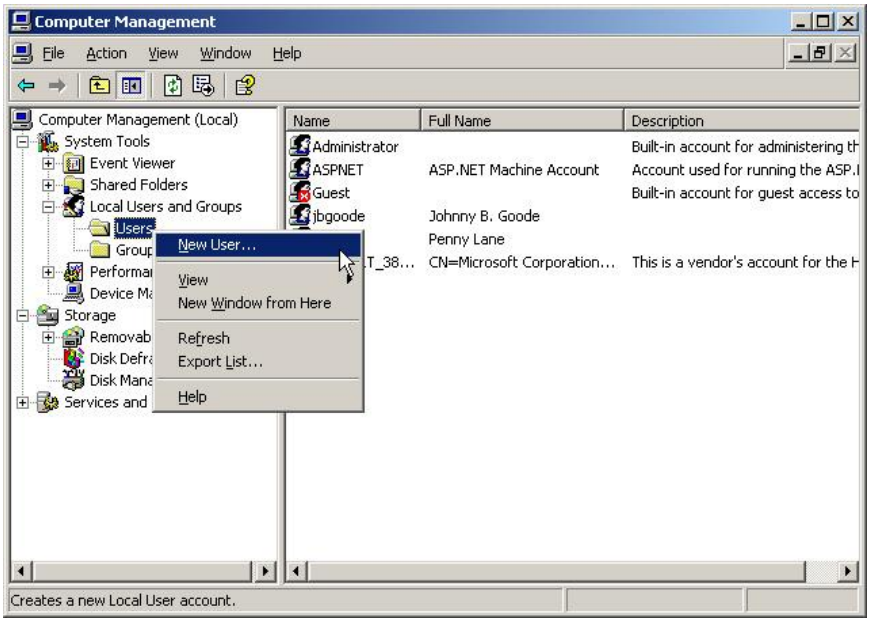


9. Assign logon rights and privileges to the new user as explained in the Configuring User Rights subsection of this document. These procedures may be used by authorized administrators to modify user logon rights and privileges at any time by adding or deleting logon rights and privileges as required.

Add a local user account to a Windows Server 2003 stand-alone or member server as follows:

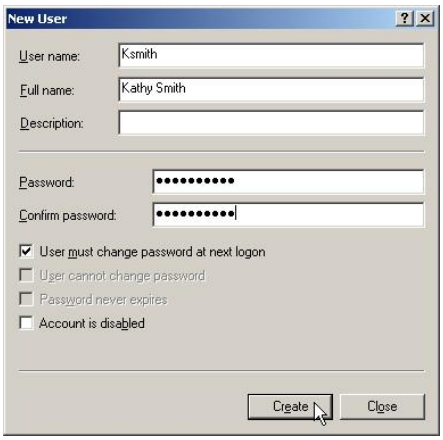
1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand **Local Users and Groups**.
4. Right-click on **Users** and select **New User**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. In the New User interface, enter a login name for the user in the **User name** text box. Enter the full name for the user in the **Full name** text box and, if desired, a description for the user account in the **Description** text box.

6. Enter an initial login password for the user in the **Password** text box and confirm the password by entering it again the **Confirm password** text box. For the Evaluated Configuration, passwords must be eight (8) characters in length or greater. If the password complexity requirements security policy has been implemented, the password must not contain all or part of the user's account name, and must contain characters from at least three (3) of four (4) classes; English Upper Case Letters, English Lower Case Letters, Base ten digits, and/or special characters (e.g., !,$,#,%). Make sure the **User must change password at next logon** box is checked to force users initially logging on to create a new password that is not known to administrators. Click the **Create** button to create the account.



7. The New User interface will clear in preparation for creating another user. If there are no other user accounts to be created, click the **Close** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Deleting a User Account

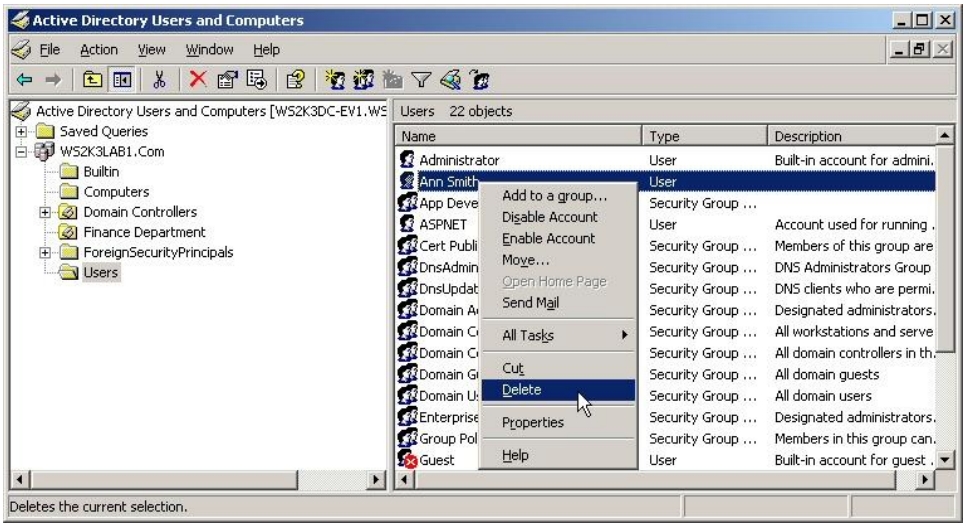
Warning: Each user account that is created has a unique, non-reusable SID. Windows Server 2003 uses the SID to identify the user and the permissions that are assigned to that user. When a user account is deleted, Windows Server 2003 does not use the SID again, even if a new user is created with the same name as the one that was deleted. Therefore, simply re-creating a deleted user account cannot restore access to resources.

User accounts can be deleted as follows:

1. Log on as an authorized administrator.

Note: The procedures below are for domain-based accounts. The procedures are similar when removing accounts from local groups on Windows Server 2003 stand-alone or member servers.

2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, click **Users**. Or, click the container that holds the user account.
4. Right-click the user account, and then click **Delete**.



5. A confirmation window will appear. Click **Yes** to delete the account.

Note: If a user is logged on to the network when that user's account is deleted, the user will retain access to the network until logged off.

Resetting a User Password

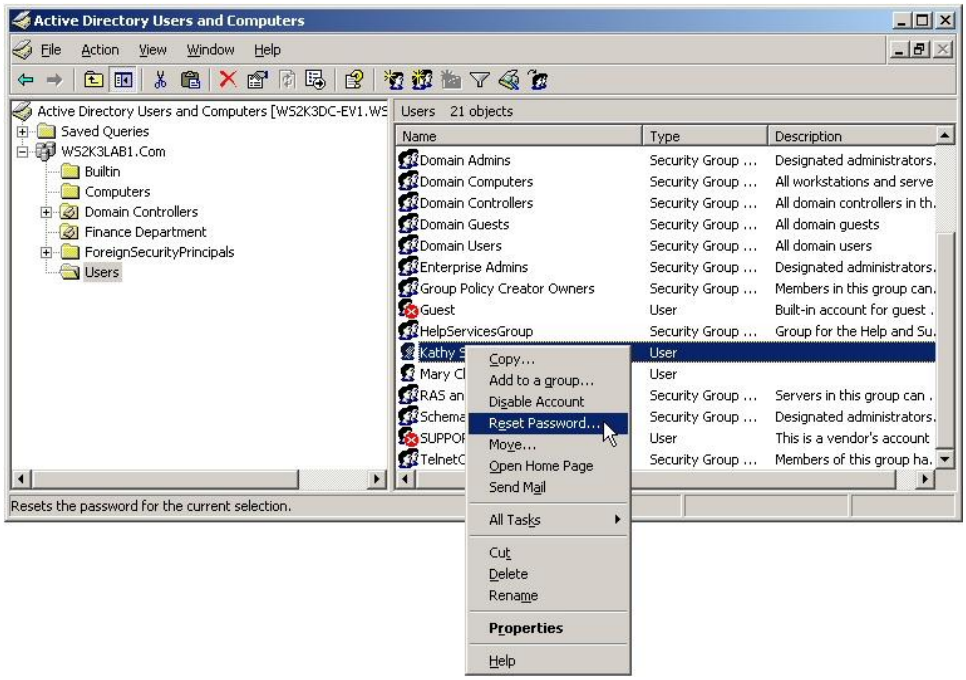
Users have the ability to change their own password if allowed to do so by the administrators. This requires that the user enter the old password for verification prior to being allowed to make the password change. However, in cases where the user does not remember the old password it will be necessary for the administrator to reset the password. To reset a user password, an authorized administrator does not need to know the old password. To ensure password security however, it is recommended that when the password is reset by an administrator, the account should be set to require the user to change the password at the next login. This will ensure that the working account password is only known by the user.

To reset a user password for a domain account:

1. Log on as an authorized administrator.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
3. In the console tree, click **Users**. Or, click the folder that contains the desired user account.
4. In the details pane, right-click the user whose password needs to be reset, and then click **Reset Password**.



5. Enter a password in the **New password** textbox and confirm the password by entering it again in the **Confirm password** textbox. To require the user to change this password at the next logon process, select the **User must change password at next logon** check box. Click **OK**.

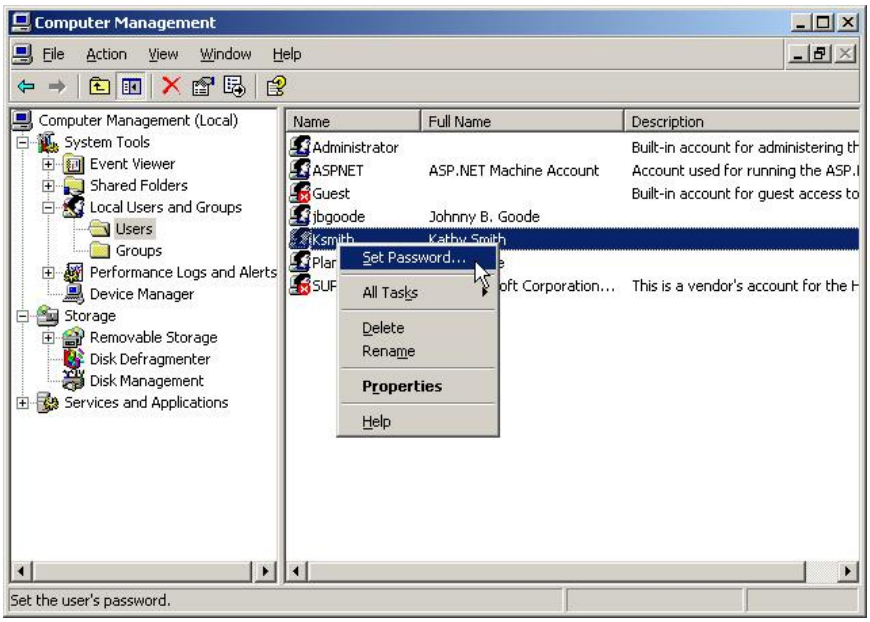
6. If the new and confirm passwords entered do not match, an error message will appear. Click **OK** and try again.
7. A verification message will appear indicating that the password has been changed. Click **OK**.

To reset a user password on a Windows Server 2003 stand-alone or member server:

1. Log in as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Computer Management**.

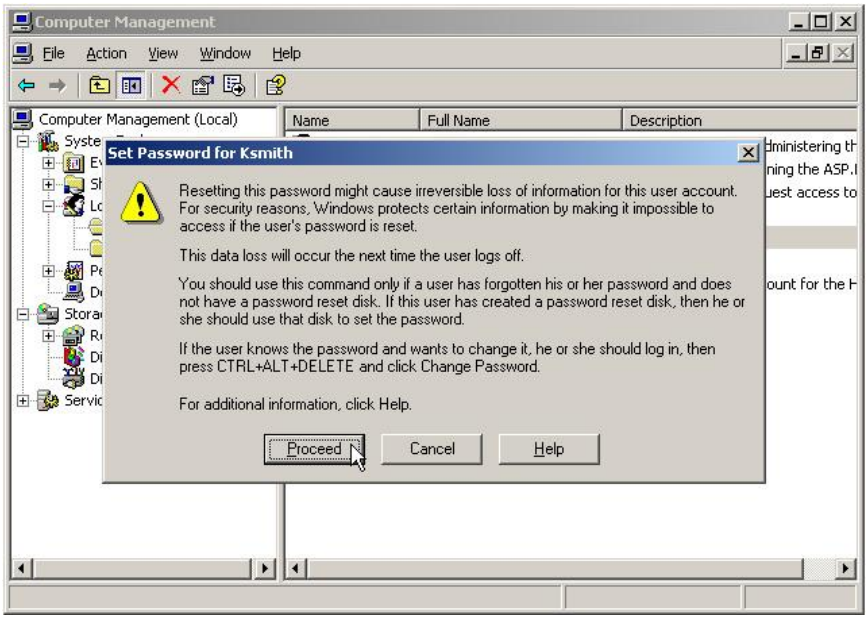
Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. Expand **Local Users and Groups**, and select the **Users** folder to view the user accounts in the right-hand pane.
4. In the details pane, right-click the user whose password needs to be reset, and then select **Set Password**.



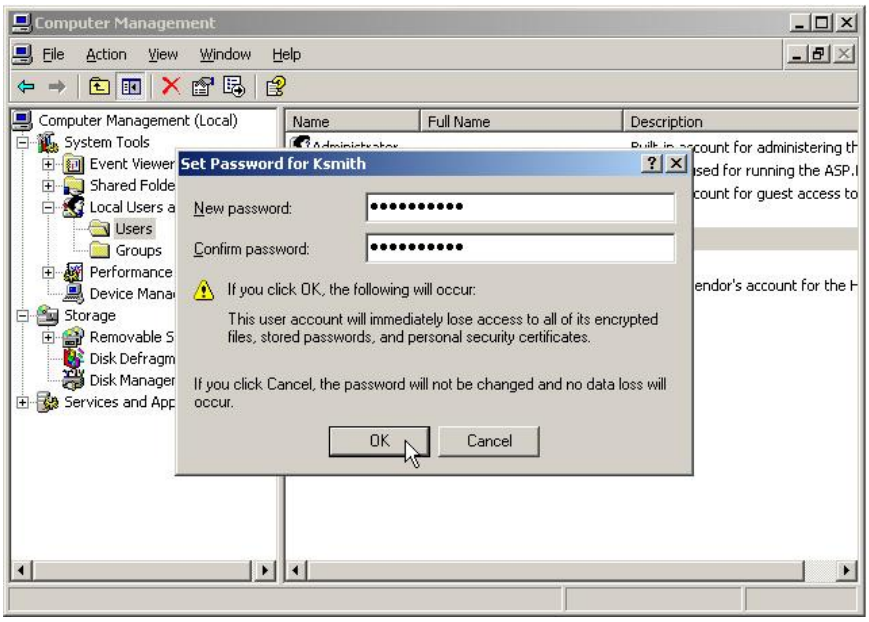
5. A warning message will appear stating that changing the password may cause irreversible loss of data. This may occur if the user has saved information in encrypted form. The administrator should verify with the user whether there is encrypted information that needs to be recovered before the password is reset by the administrator. If there is, it may be recoverable using a Data Recovery Agent (DRA). See procedures for using a Data Recovery Agent before proceeding. If it is OK to proceed, click the **Proceed** button.

Note: Password changes made by administrators to Domain-level user accounts are not affected by loss of access to encrypted files as are local accounts.



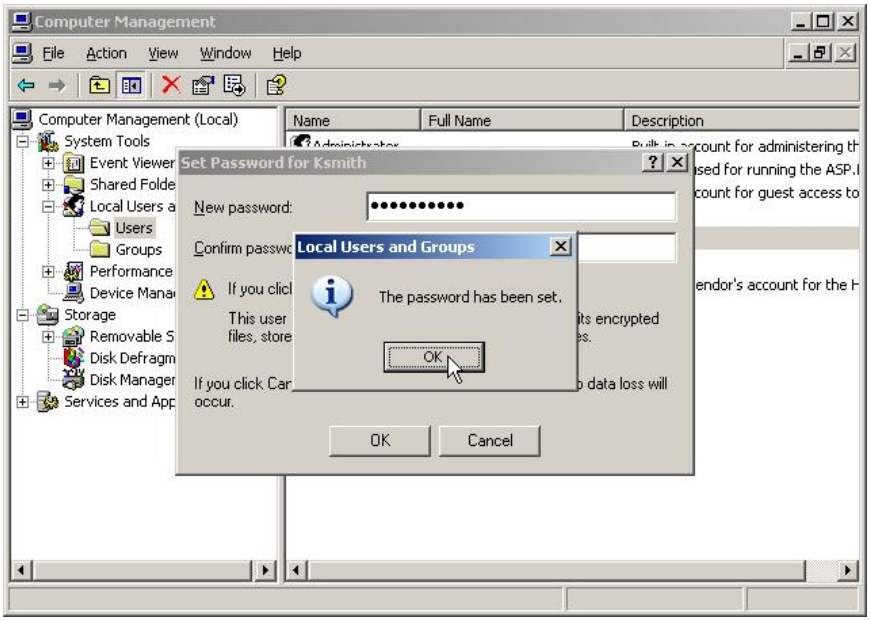
Copyright © 2008 Microsoft Corporation.
All rights reserved.

6. On the **Set Password for <*username*>** interface, there will be a second warning about potential loss of data. Enter a password in the **New password** textbox and confirm the password by entering it again in the **Confirm password** textbox. Click **OK**.



7. If the new and confirm passwords entered do not match, an error message will appear. Click **OK** and try again.

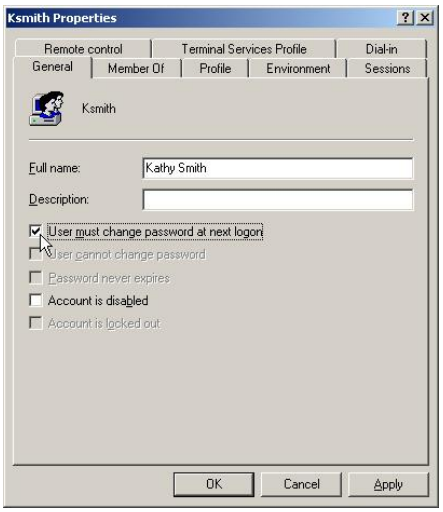
8. Once the new password has been entered and correctly confirmed, a message will appear stating that the password has been set. Click **OK**.



9. To require the user to change this password at the next logon process, double-click the user account or right-click and select **Properties**. The account **Properties** window will appear. Within the General tab view, check the **User must change password at next logon** check box. Click **OK** to close the **Properties** window.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

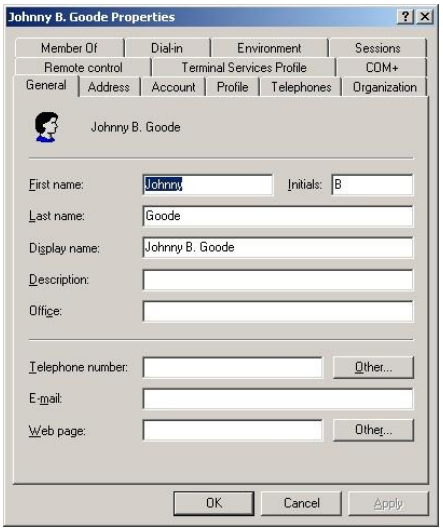


Modifying Account Properties

The **Properties** interface for each account contains a set of tabs that allows administrators to configure various properties for a specific user. A set of default properties is associated with each domain user account and local user account created. Domain user accounts contain more properties than local user accounts. Local user account properties represent a very small subset of domain user account properties.

Domain user accounts can be modified by:

1. Opening the **Active Directory Users and Computers** snap-in.
2. Selecting the folder containing the account to be modified.
3. In the details pane, double-clicking on the user object whose properties are to be modified (or right-clicking on the user object and selecting **Properties**. The following **Properties** interface will appear for domain user accounts:



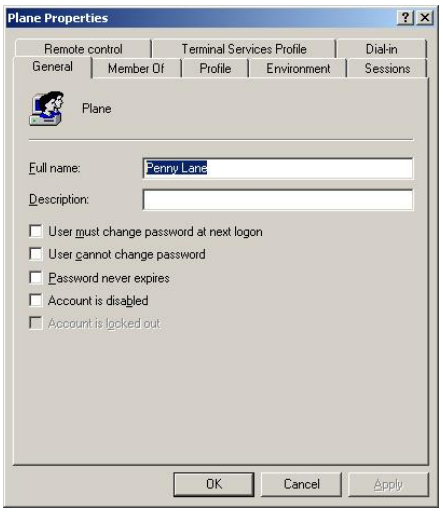
Properties that are defined for a domain user account can be used to search for users in the Active Directory store. For example, if a user knows a person's first name and telephone number and wants to find the person's last name, the user can enter the telephone number to search for the last name.

Local user accounts can be modified by:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

1. Opening the **Computer Management** snap-in Windows Server 2003 stand-alone or member servers.
2. Expanding the **Local users** and **Groups** folder.
3. Selecting the **Users** folder, and double clicking on the user object whose properties are to be modified (or right clicking on the user object and selecting **Properties**. The following **Properties** interface will appear for local user accounts:



The Properties interface

The table below describes each of the account properties tabs that can be modified. The descriptions in apply to domain and/or local accounts as specified.

Tab	Description
Account (Domain)	Allows setting a user's logon name and other account options for the user account. Some of these options were set as default when the user account was created in Active Directory. The defaults can be modified and additional settings can be configured.
Address (Domain)	Use this tab to document the user's street address, post office box, city, state or province, zip code, and country.
COM+ (Domain)	Allows authorized administrators to make the user a member of a particular COM+ partition set.
Dial-in (Domain & Local)	Allows for controlling how a user can make a dial-in connection to the network from a remote location.
Environment (Domain & Local)	Allows authorized administrators to configure the Terminal Services startup environment.
General (Domain)	Use this tab to document the user's name, description, office location, telephone, e-mail, and home page information.
General (Local)	Use this tab to document the user's full name and description. Also allow authorized administrators to force users to change their password at next logon, keep users from changing their passwords, set passwords to never expire, disable an account, or unlock an account that has been locked due to repeated login failures.
Member of (Domain & Local)	Allows modification of group membership for users.

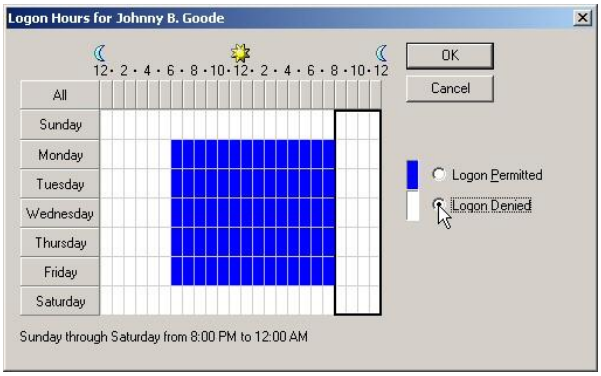
Copyright © 2008 Microsoft Corporation.
All rights reserved.

Tab	Description
Organization (Domain)	Use this tab to document the user's title, department, company manager, and direct reports.
Profile (Domain & Local)	User profiles automatically create and maintain the desktop settings for each user's work environment on the local computer. Allows setting a path where the user profiles are to be stored, assigning logon scripts and setting a home folder.
Remote Control (Domain & Local)	Allows authorized administrators to configure remote control setting to remotely control or observe a user's session.
Sessions (Domain & Local)	Allows authorized administrators to configure Terminal Services timeout and reconnection settings.
Telephones (Domain)	Used this tab to document the user's home, pager, mobile, fax, and IP telephone numbers, and to add comments.
Terminal Service Profile (Domain & Local)	Allows users to log on from a computer terminal and run Windows Server 2003 sessions on the terminal.

Configuring Logon Hours

To configure the logon hours, follow these steps:

1. Log on to the Domain Controller as an authorized administrator.
2. Access the user's **Properties** interface in **Active Directory Users And Computers** and then choose the **Account** tab.
3. Click the **Logon Hours** button. Set the valid and invalid logon hours using the **Logon Hours** interface shown. In this interface each hour of the day or night is a field that can be turned on or off. To change the setting for an hour, select it. Then select either the **Logon Permitted** or **Logon Denied** option button.
   - Hours that the user is allowed to log on are filled in with a blue bar.
   - Hours that the user is not allowed to log on are blank.



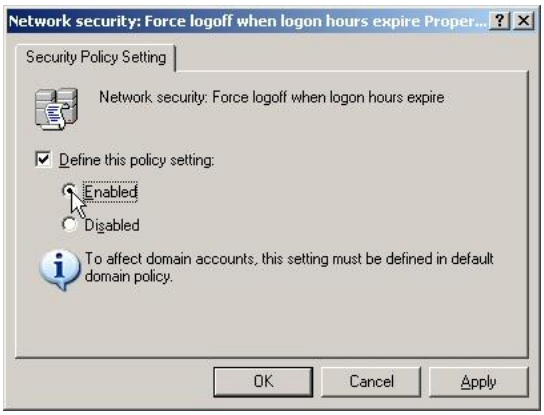
4. To ensure that logon restrictions are verified prior to allowing a user to log on, review the **Enforce user logon restrictions** setting of the **Kerberos Policy** to verify that it is enabled as described in the Configuring Kerberos Policies subsection.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Automatically Log Off Users when Logon Time Expires

To forcibly disconnect users when their logon time has expired, as set in the previous subsection, follow these steps:

1. To forcibly disconnect users who are members of a domain, access the **Domain Security Policy** interface and follow the procedures in the Configuring Security Options subsection to expand **Local Policies** and access the **Security Options**.
2. Double click on the **Network security: Force logoff when hours expire** option, or right-click on it and select **Properties**. This opens a **Properties** interface for the selected option.
3. Check **Define this policy setting** and select the **Enabled** radio button.



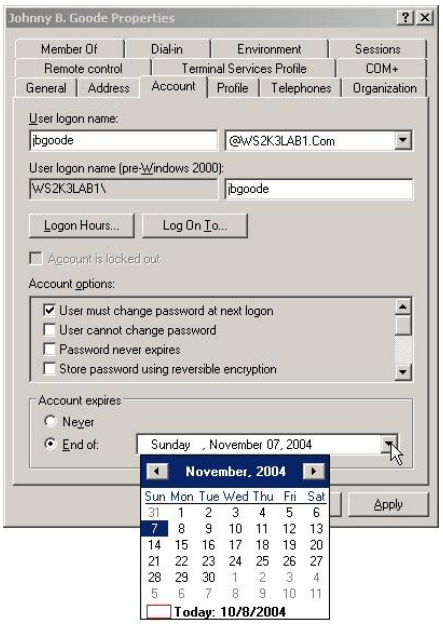
4. Click **OK** to configure the selected option.

Set an Account Expiration Date

To configure an account expiration date for a user account, follow these steps:

1. Access the user's **Properties** interface in **Active Directory Users And Computers** and then choose the **Account** tab.
2. Under **Account expires**, select the **End of:** radio button.
3. In the date drop down menu box, select the drop down arrow. A calendar window will appear showing the current date. Use the calendar to select the date the account is to expire on by using the forward arrow (right side arrow) to select a future month, and then clicking on the desired day within the calendar.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

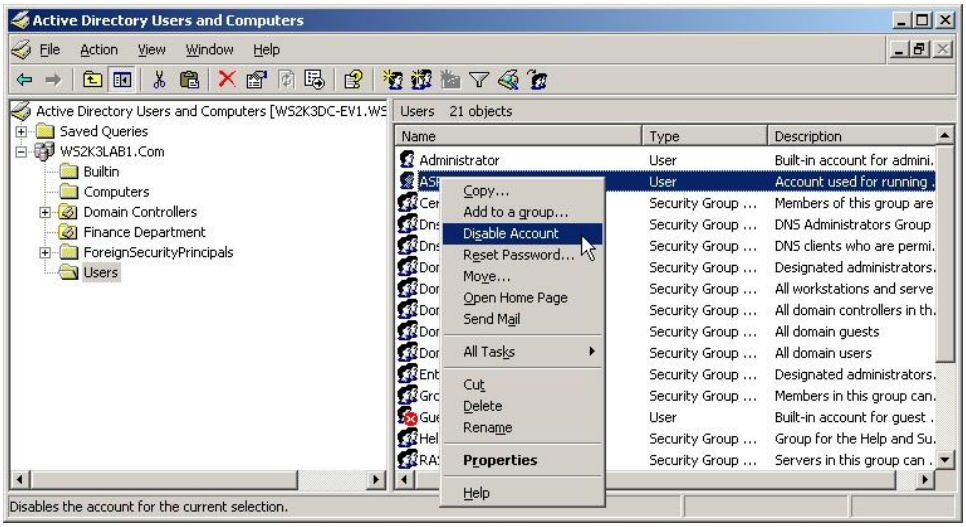


4. Click the **Apply** button and click **OK** to close user's the **Properties** interface.

Disabling and Enabling User Accounts

To disable a user account within a domain, follow these steps:

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Users and Computers**.
3. In the console tree, click **Users** or the folder that contains the desired user account.
4. In the details pane, right-click the user.
5. Click **Disable Account** as shown below.

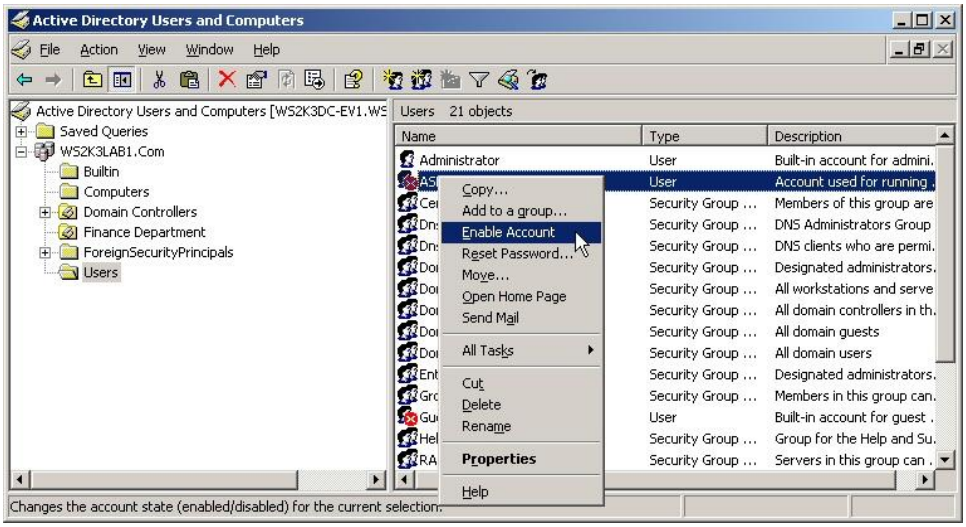


6. A message will appear indicating that the account has been disabled. Click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

To enable a user account that has been disabled within a domain:

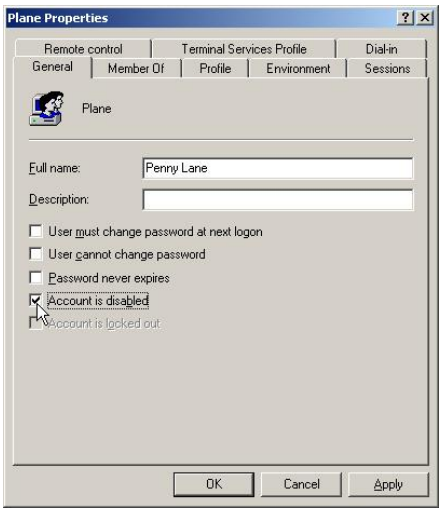
1. Right-click the user account in **Active Directory Users and Computers**.
2. Select **Enable Account**.



3. A message will appear indicating that the account has been enabled. Click **OK**.

To disable a local user account on a Windows Server 2003 stand-alone or member server, follow these steps:

1. Log in as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand **Local Users and Groups**, and select the **Users** folder to view the user accounts in the right-hand pane.
4. In the details pane, right-click the user whose account needs to be disabled, and then select **Properties**.
5. In the **General** tab of the account **Properties** interface, check the **Account is disabled** box.



6. Click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

To enable a local user account that has been disabled on a Windows Server 2003 stand-alone or member server

1. Open the user's Properties interface in **Computer Management**.
2. Uncheck the **Account is disabled** box and click **OK**.

Data Protection

Information security strategies protect data on servers and client computers, and also conceal and protect packets traversing insecure networks. Distributed security plans need to identify which information must be protected in the event computer equipment is lost or stolen. Also, types of network traffic that are sensitive or private and need to be protected from network sniffers must be included in the plan.

In terms of users on the enterprise network, access control is the primary mechanism to protect sensitive files from unauthorized access. However, the computers themselves might be portable and subject to physical theft. Therefore, access control is not sufficient to protect the data stored on these computers. This is a special problem with laptop computers that can be easily stolen while traveling. Windows Server 2003 provides EFS to address this problem.

To keep network data packets confidential, IPSec can be used to encrypt network traffic among some or all of the servers in an organization. IPSec provides the ability to set up authenticated and encrypted network connections between two computers. For example, an e-mail server can be configured to require secure communication with clients and thereby prevent a packet sniffer from reading e-mail messages between the clients and the server. IPSec is ideal for protecting data from existing applications that were not designed with security in mind.

Hardware Data Execution Prevention (DEP) Settings on 64-bit Operating Systems

This subsection defines procedures for verifying hardware DEP support on platforms hosting the Windows Server 2003 64-bit edition operating systems. On 64-bit editions of Windows, hardware-enforced DEP is automatically enabled for all 64-bit processes and there are no system configuration settings to disable this. However, DEP support for 32-bit processes running on a 64-bit version of Windows is configurable. The **Windows Management Instrumentation Command-line (WMIC)** tool may be used by authorized administrators to verify whether or not hardware-enforced DEP is supported by the hardware and if the OS is using it. The **WMIC** tool also returns information about the current DEP configuration for 32-bit processes that are running on 64-bit operating systems by providing administrators with data indicating which system-wide DEP configuration for 32-bit processes is enabled. DEP protection for 32-bit processes that are running on 64-bit operating systems is controlled by using the **Data Execution Prevention** performance option of the **System Properties** interface.

Verify use of hardware DEP

Authorized administrators may use the **WMIC** tool to determine if the hardware supports DEP and to determine if a Windows Server 2003 64-bit edition operating system is configured to support DEP for 32-bit binaries. If the hardware supports DEP, it will be used by default by the 64-bit operating system and all 64-bit processes. DEP cannot be disabled for 64-bit operating systems and processes.

To determine if the current hardware supports DEP:

1. Click **Start**, and select **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**. A command line interface will appear.
3. At the command prompt, type the following command, and then press **ENTER**:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

wmic OS Get DataExecutionPrevention_Available

Note: If this is the first time WMIC is executed on the computer, a brief message is displayed stating Please wait while wmic is being installed. Then the results of the command are displayed.

4. If the output is **TRUE**, hardware-enforced DEP is available.

To verify that Windows is running with hardware-enforced DEP enabled:

5. Click **Start**, and select **Run**.
6. Type **cmd** in the **Open** box, and then click **OK**. A command line interface will appear.
7. At the command prompt, type the following command, and then press **ENTER**:

wmic OS Get DataExecutionPrevention_Drivers

8. If the output is **TRUE**, Windows is using hardware-enforced DEP.

To use WMIC to determine if DEP is being used for 32-bit binaries:

1. Click **Start**, and select **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**. A command line interface will appear.
3. At the command prompt, type the following command, and then press **ENTER**:

wmic OS Get DataExecutionPrevention_SupportPolicy

4. The value returned is 0, 1, 2 or 3. This value corresponds to one of the DEP support policies described in the table below.

Data Execution Prevention Support Policy Property Value	Policy Level	Description
2	OptIn	Only 32-bit Windows core binaries and processes have DEP protection.
3	OptOut	DEP is enabled for all 32-bit processes. Administrators can manually create an exclusion list of specific programs to exclude from DEP protection.
1	AlwaysOn	DEP is enabled system-wide for all 32-bit processes.
0	AlwaysOff	DEP is not enabled for any 32-bit processes.

Configure use of hardware DEP for 32-bit processes

DEP protection for 32-bit processes that are running on 64-bit operating systems is controlled by using the **Data Execution Prevention** performance option of the **System Properties** interface. There are two system-wide configurations options available through the **System Properties** interface:

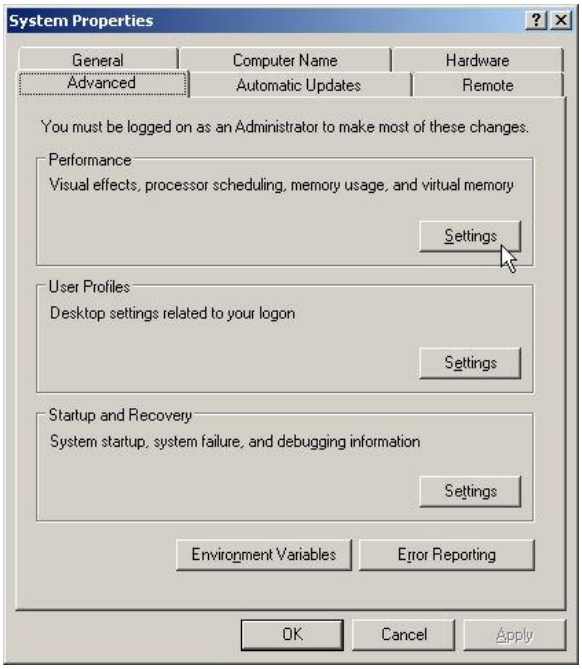
- **OptIn**. This option enables DEP only for Windows core binaries and processes. **OptIn** is the default configuration for computers running Windows XP.
- **OptOut**. This option enables hardware-enforced DEP for all 32-bit processes. **OptOut** is the default configuration for computers running Windows Server 2003. The administrator can exclude the use of hardware-enforced DEP for specific 32-bit programs by adding them to the exception list.

To modify hardware-enforced DEP option for 32-bit processes:

1. Click **Start**, right-click on **My Computer**, and select **Properties**. The **System Properties** interface will appear.
2. Click the **Advanced** tab, and then under **Performance**, click the **Settings** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



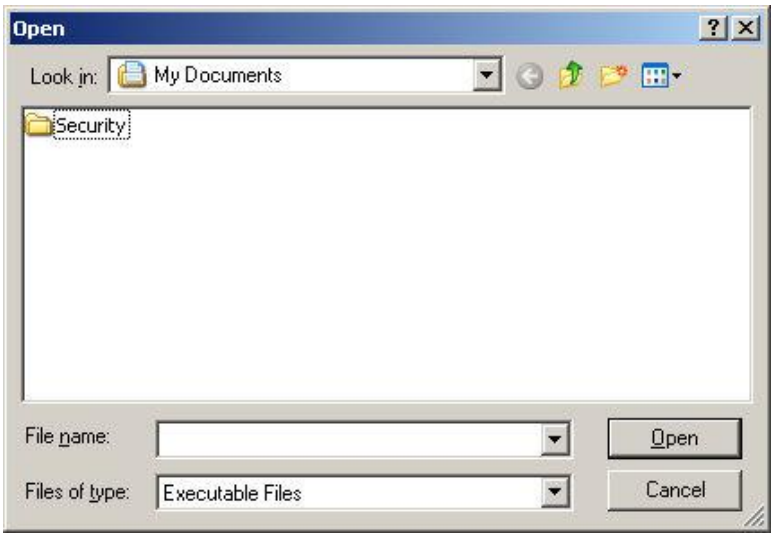
3. Click the **Data Execution Prevention** tab in the **Performance Options** interface.

4. By default, the **Turn on DEP for all programs and services except those I select** radio button is selected on Windows Server 2003 operating systems. This sets the **OptOut** system-wide configurations option and enables hardware-enforced DEP for all 32-bit processes.

5. To exclude the use of hardware-enforced DEP for specific programs, click the **Add** button. Search for the program that is to be excluded by navigating the file system with the **Open** interface.

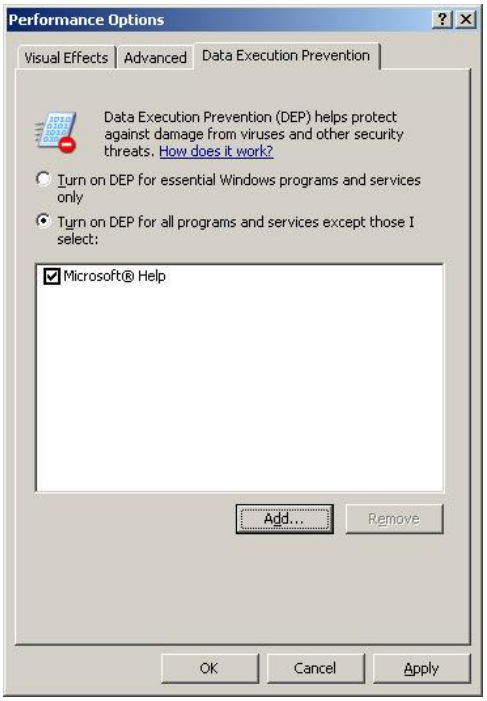
Copyright © 2008 Microsoft Corporation.

All rights reserved.



6. Select the desired program file and click the **Open** button. A warning message will be displayed. Click **OK**.

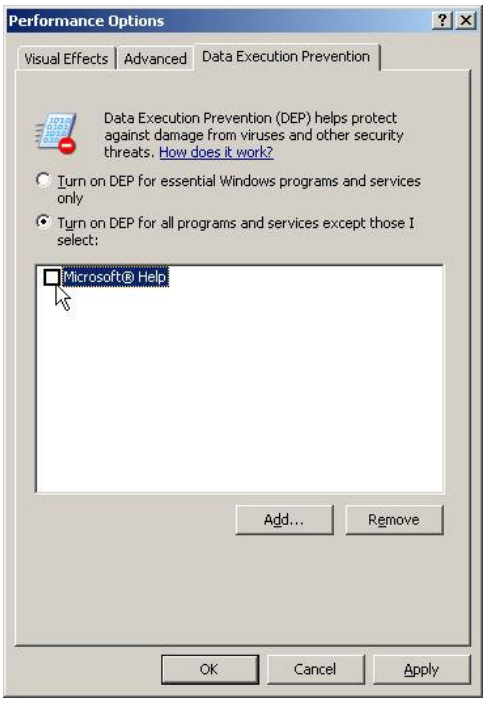
7. The selected program will appear in the exclusion window. Once all programs that are to be excluded have been selected, click the **OK** button on the **Performance Options** interface.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

8. In some cases, a message will appear indicating that the computer will need to be restarted before the changes can take effect.

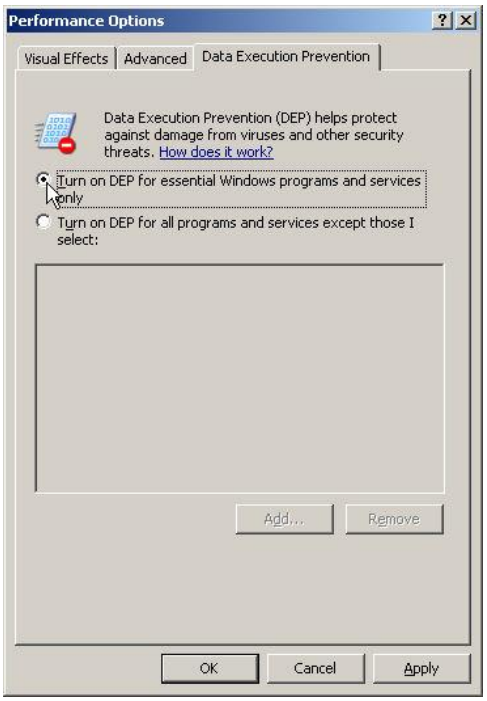
9. To remove a previously excluded program from the hardware-enforced DEP exclusion list, uncheck the box next to the program.



10. To enable DEP only for Windows core binaries and processes, select the **Turn on DEP for essential Windows programs and services** radio button. This sets the **OptIn** system-wide configurations option for DEP. Click the **OK** button on the **Performance Options** interface.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



11. A message will appear indicating that the computer will need to be restarted before the changes can take effect. Click **OK** and restart the computer.

Setting Access Controls on Files, Folders, Shares, and Other System Objects

Access control is the process of authorizing access to users and groups, and the ability to perform specific actions, to objects on the network and the local computer. Key concepts that make up access control are described below.

- **Least Privilege Principle:** A key component of authorization is the least privilege principle, which states that all users should have the least possible amount of systems access that still allows them to perform their job functions. Thus, if a user only needs to be able to view a particular file, that user should have read-only access to the file; the user should not be able to write to that file.
- **Ownership of Objects:** Windows Server 2003 assigns an owner to an object when the object is created. By default, the owner is the creator of the object.
- **Permissions Attached to Objects:** The primary means for access control is permissions, or access rights. In Windows systems, permissions can be set on files, folders, and other objects within the system. Permissions allow or deny users and groups particular actions for users and groups. Permissions are implemented primarily by way of security descriptors, which also define auditing and ownership. An example of a permission attached to an object is Read permission on a file. When first installing a Windows system, make sure system object permissions are properly set. In some cases, the system defaults to least privilege; in other cases it may not. Determining whether system permissions conform to the least privilege principle, and modifying those which do not, is called hardening the operating system. This should be done as part of the initial system installation process.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- **Inheritance of Permissions:** Windows Server 2003 provides a feature for administrators to easily assign and manage permissions. Known as inheritance, this feature automatically causes objects within a container to inherit the permissions of that container. For example, the files within a folder, when created, inherit the permissions of the folder.
- **Object Managers:** If there is a need to change the permissions on an individual object, the appropriate tool must be used to change the properties for that object. For example, to change the permissions on a file, start **Windows Explorer**, right-click on the file name, and click **Properties**. This interface can be used to change permissions on the file.
- **Object Auditing:** Windows Server 2003 allows the administrator to audit users' access to objects. These security-related events can be viewed in the security log with the **Event Viewer**.

Security Descriptors

Access control permissions are assigned to shared objects and Active Directory objects to control how different users can use each object. A shared object, or shared resource, is an object that is intended to be used over a network by one or more users and includes files, printers, folders, and services. Both shared objects and Active Directory objects store access control permissions in security descriptors.

A security descriptor contains two Access Control Lists (ACLs) used to assign and track security information for each object: the DACL and the system access control list (SACL).

- **DACLs**. DACLs identify the users and groups that are assigned or denied access permissions on an object. If a DACL does not explicitly identify a user, or any groups that a user is a member of, the user will be denied access to that object. By default, a DACL is controlled by the owner of an object or the person who created the object, and it contains Access Control Entries (ACEs) that determine user access to the object. An ACE is an entry in an object's DACL that grants permissions to a user or group. An ACE is also an entry in an object's SACL that specifies the security events to be audited for a user or group.
- **SACLs**. SACLs identify the users and groups that are to be audited when they successfully access or fail to access an object. Auditing is used to monitor events related to system or network security, to identify security breaches, and to determine the extent and location of any damage. By default, a SACL is controlled by the owner of an object or the person who created the object. A SACL contains ACEs that determine whether to record a successful or failed attempt by a user to access a object using a given permission, for example, Full Control and Read.

Copying vs. Moving

When using NTFS permissions to secure access to specific files or folders, it is very important to pay close attention to what happens to those permissions whenever the object is moved or copied to another location on the system:

- When an object is copied into another directory it inherits the access privileges in place at the destination folder.
- When a file or directory object is moved from one directory to another directory, the NTFS permissions that have been applied to the file move with it.

File Permissions

File permissions include Full Control, Modify, Read & Execute, Read, and Write. Each of these permissions consists of a logical group of special permissions. The following table lists NTFS file permissions and specifies which special permissions are associated with that permission.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

	NTFS File Permissions				
Special Permissions	**Full Control**	**Modify**	**Read & Execute**	**Read**	**Write**
Traverse Folder/Execute File	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permissions	✓	✓	✓	✓	✓
Change Permissions	✓				
Take Ownership	✓				

Warning: Groups or users granted Full Control on a folder can delete any files in that folder regardless of the permissions protecting the file.

Folder Permissions

Folder permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Each of these permissions consists of a logical group of special permissions. The following table lists NTFS folder permission and specifies which special permissions are associated with that permission.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

	Folder Permissions					
Special Permissions	**Full Control**	**Modify**	**Read & Execute**	**List Folder Contents**	**Read**	**Write**
Traverse Folder/Execute File	✓	✓	✓	✓		
List Folder/Read Data	✓	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	✓	
Create Files/Write Data	✓	✓				✓
Create Folders/Append Data	✓	✓				✓
Write Attributes	✓	✓				✓
Write Extended Attributes	✓	✓				✓
Delete Subfolders and Files	✓					
Delete	✓	✓				
Read Permissions	✓	✓	✓	✓	✓	✓
Change Permissions	✓					
Take Ownership	✓					

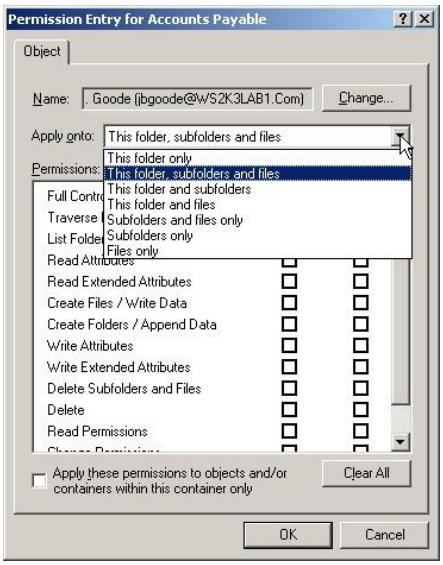
Although **List Folder Contents** and **Read & Execute** appear to have the same special permissions, these permissions are inherited differently. **List Folder Contents** is inherited by folders but not files, and it should only appear when viewing folder permissions. **Read & Execute** is inherited by both files and folders and is always present when viewing file or folder permissions.

Selecting where to Apply Permissions

The **Permission Entry** interface appears when permissions are set on files and folders. In this interface, **Apply onto** lists the locations where permissions can be applied. How these permissions are applied depends on whether the **Apply these permissions to objects and/or containers within this container only** check box is selected. By default, this check box is clear.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



When the **Apply these permissions...** check box is clear, permissions are applied as shown below:

Apply onto	Applies permissions to current folder	Applies permissions to subfolders in current folder	Applies permissions to files in current folder	Applies permissions to all subsequent subfolders	Applies permissions to files in all subsequent subfolders
This folder only	✓				
The folder, subfolders and files	✓	✓	✓	✓	✓
This folder and subfolders	✓	✓		✓	
This folder and files	✓		✓		✓
Subfolders and files only		✓	✓	✓	✓
Subfolders only		✓		✓	
Files only			✓		✓

Copyright © 2008 Microsoft Corporation.
All rights reserved.

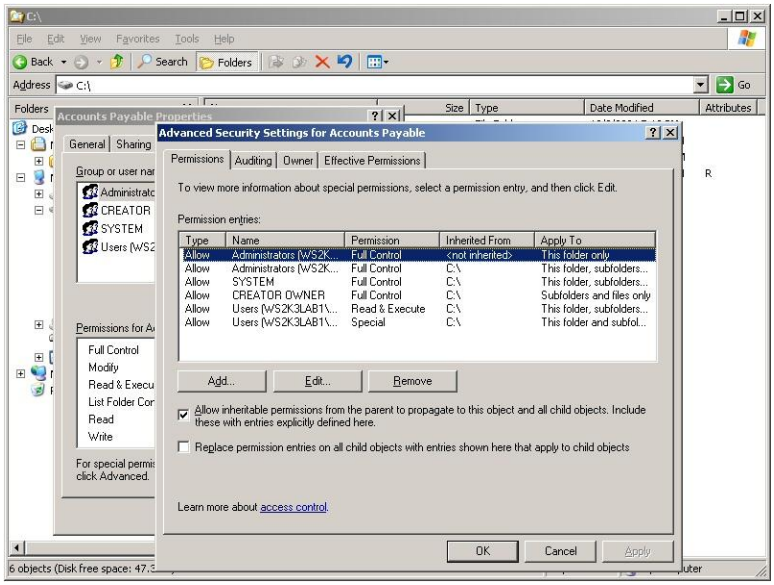
When the **Apply these permissions...** check box is selected, permissions are applied as shown below:

Apply onto	Applies permissions to current folder	Applies permissions to subfolders in current folder	Applies permissions to files in current folder	Applies permissions to all subsequent subfolders	Applies permissions to files in all subsequent subfolders
This folder only	✓				
The folder, subfolders and files	✓	✓	✓		
This folder and subfolders	✓	✓			
This folder and files	✓		✓		
Subfolders and files only		✓	✓		
Subfolders only		✓			
Files only			✓		

Setting or Modifying Permissions

To set, view, change, or remove special permissions for files and folders:

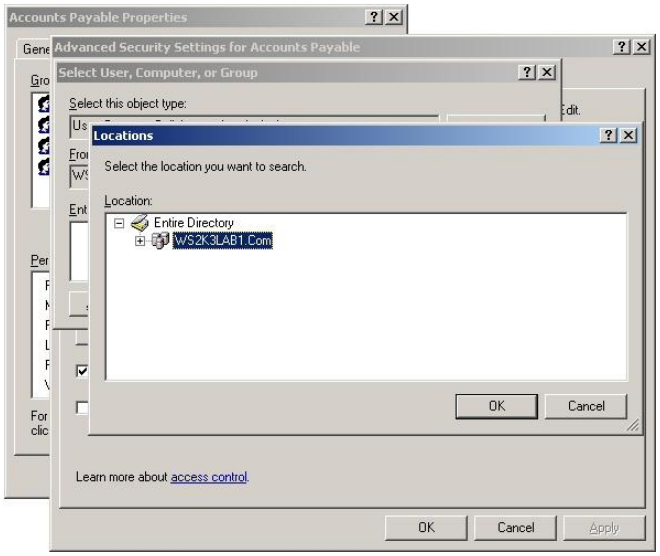
1. Open Windows Explorer; click **Start**, point to **Programs**, point to **Accessories**, and then select **Windows Explorer**.
2. Navigate **Windows Explorer** and locate the file or folder for which special permissions are to be set.
3. Right-click the file or folder, click **Properties**, and then click the **Security** tab.
4. Click **Advanced**.

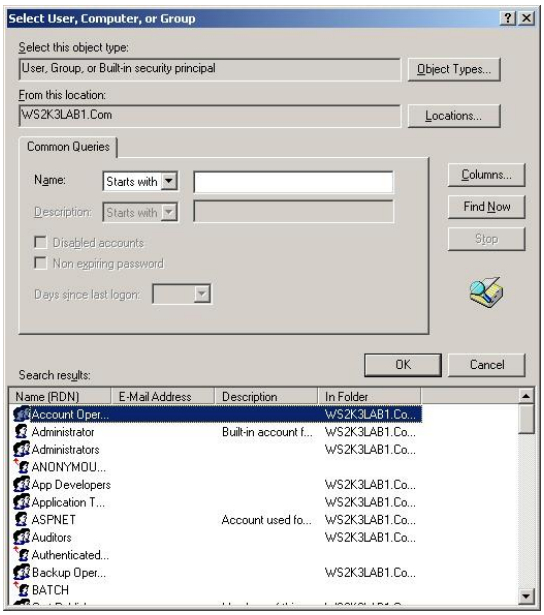


5. Perform one of the following:

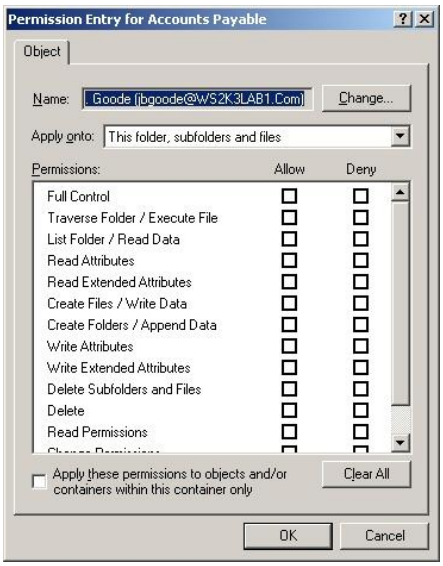
Copyright © 2008 Microsoft Corporation.
All rights reserved.

- To set special permissions for a new group or user, click **Add** to open the **Select User, Computer, or Group** interface (on a stand-alone Windows Server 2003 computer, it is the **Select User or Group** interface). Enter the name of the user or group using the format *domainname\name* or click the **Advanced** button, then the **Find Now** button to select an account name from a list. To access account names from a domain, click the **Locations** button. There should now be a list that shows the local domain, trusted domains, and other resources that can be accessed. Select the local domain to view all the account names in the domain.





- Select an account and click **OK** on the **Select User, Computer, or Group** interface. If the **Advanced** feature was used, click **OK** again in the next **Select User, Computer, or Group** interface. The **Permission Entry** interface for the selected account will appear.

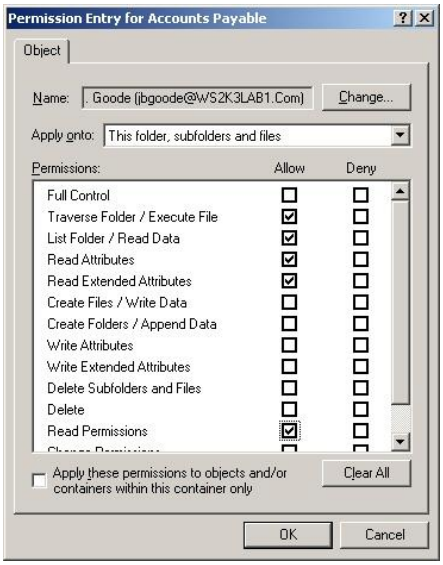


- Set permissions by checking the desired permission check boxes under the **Allow** column. To explicitly deny a permission to the account, check the appropriate check box under the **Deny** column.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: Permissions that are explicitly denied will take precedence over all others. Therefore, if the account is a member of a group that is allowed the permission as well as another group that denied the permission on the same object, the effective setting will be to **Deny** the permission.



- To view or change special permissions for an existing group or user, select the name of the account and then click **Edit**. If the permission settings are not selectable (grayed out), it is because the permissions are inherited from a parent folder. See How inheritance affects file and folder permissions for details.
- To remove a group or user and its special permissions, select the name of the account and then click **Remove**. If the **Remove** button is unavailable, it is because the permissions are inherited from a parent folder. See How inheritance affects file and folder permissions for details on how to make changes to inherited permissions.
- In the **Permission Entry for <account name>** interface, select where the permissions are to be applied, if necessary, by using the **Apply onto** drop-down menu. **Apply onto** is available only for folders.
- To prevent subfolders and files within the tree from inheriting these permissions, click to select the **Apply these permissions to objects and/or containers within this container only** check box.

Note: To change permissions, a user must be the owner or have been granted permission to do so by the owner.

Warning: Groups or users granted Full Control for a folder can delete files and subfolders within that folder regardless of the permissions protecting the files and subfolders.

How Inheritance affects File and Folder Permissions

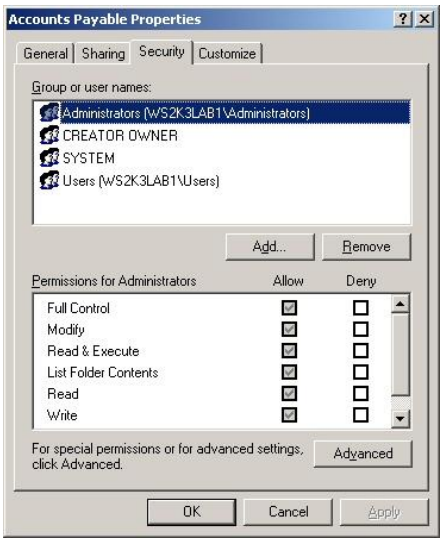
After setting permissions on a parent folder, new files and subfolders created in the folder inherit those permissions. If inherited permissions are not desired, select **This folder only** in **Apply onto** when special permissions are set for the parent folder.

To prevent only certain files or subfolders from inheriting permissions from a parent folder:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

1. Right-click the file or subfolder, select **Properties**, click the **Security** tab. If the permission check boxes for an account appear shaded, the file or folder has inherited permissions from the parent folder.

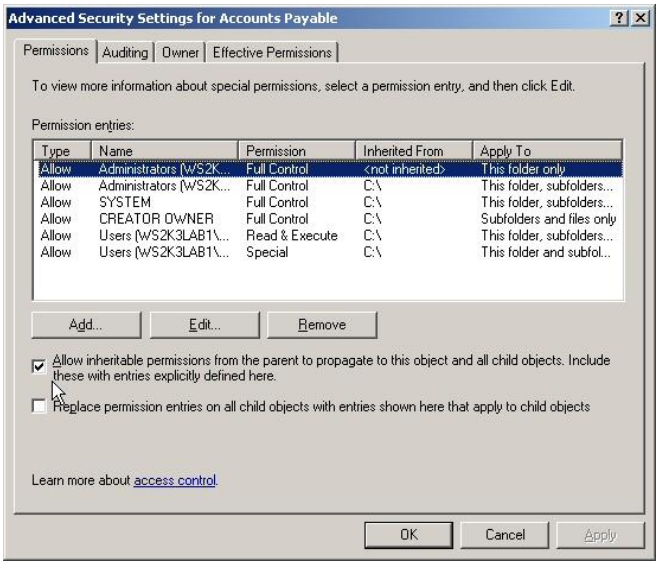


2. There are three ways to make changes to inherited permissions:
   - Make the changes to the parent folder, and then the file or folder will inherit these permissions.
   - Select the opposite permission (i.e., **Deny**) to override the inherited permission.
   - Clear the **Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here** check box. This will allow changes to the permissions or removal of the user or group from the permissions list. However, the file or folder will no longer inherit permissions from the parent folder.
3. To clear the inheritance of permissions from a parent folder, click the **Advanced** tab on the **Properties** interface and uncheck the **Inherit from parent the permission entries that apply to child objects…** check box.

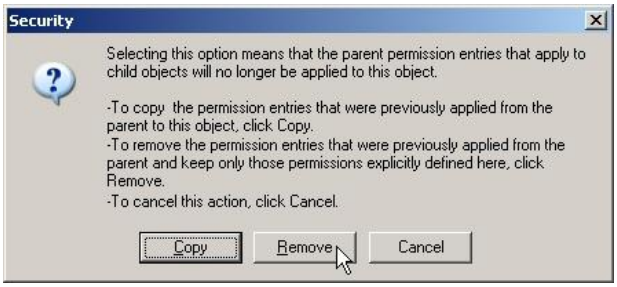
Note: On Domain Controllers, **Full Control** permissions for the **Administrators** group are applied directly to a newly created file or folder. These permissions are not inherited as shown in the **Advanced Security Settings for <*file or folder name*>** interface below.

Copyright © 2008 Microsoft Corporation.

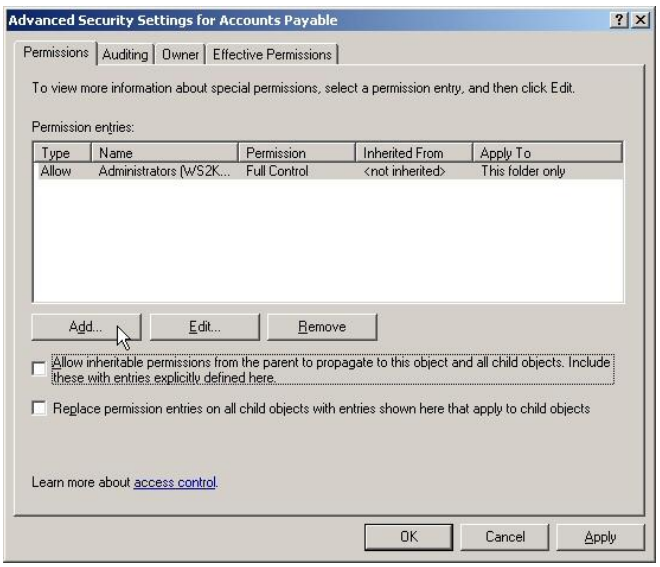
All rights reserved.



4. A **Security** message interface, shown below, will appear asking whether to copy inherited permissions or remove them. If the **Copy** button is clicked, inheritance is removed and the permissions previously inherited are copied to the object. The copied permissions can then be modified. If the **Remove** button is clicked, all inherited permissions are removed. Click on the **Remove** button.



5. All permissions previously inherited are removed from the file or subfolder. If there are no locally applied permissions, or if additional permissions are required, the new permissions must now be added to allow appropriate access.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

6. Click the add button to add and modify permissions as previously described above in Setting or modifying permissions.

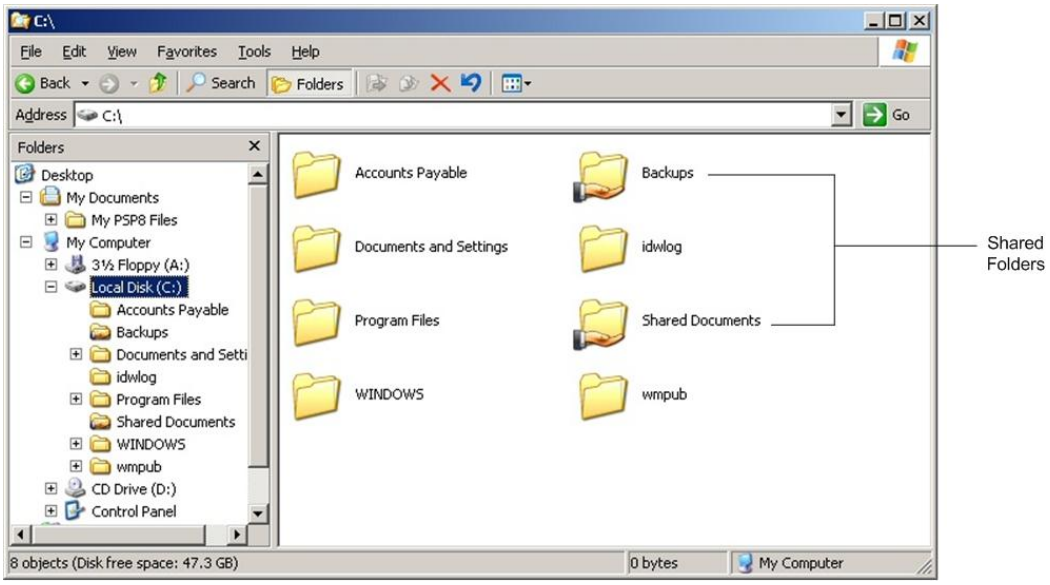
Shared Folder Permissions

Shared folders are used to provide network users with access to files and application resources on the network. When a folder is shared, users can connect to the folder over the network and gain access to the files that it contains. However, to gain access to the files, users must have permissions to access the shared folders.

A shared folder can contain applications, data, or a user's personal data, called a home folder. Each type of data requires different shared folder permissions. The following are characteristics of shared folder permissions:

- Shared folder permissions apply to folders, not individual files. Since shared folder permissions can be applied only to the entire shared folder, and not to individual files or subfolders in the shared folder, shared folder permissions provide less detailed security than NTFS permissions.
- Shared folder permissions do not restrict access to users who gain access to the folder at the computer where the folder is stored. They apply only to users who connect to the folder over the network.
- Shared folder permissions are the only way to secure network resources on a File Allocation Table (FAT) volume. NTFS permissions are not available on FAT volumes.
- On an NTFS volume, share permissions control access to the location of resource objects and NTFS permissions provide additional access restrictions to the objects within the share.

A shared folder appears in **Windows Explorer** as an icon of a hand holding the shared folder as shown below.



To control how users gain access to a shared folder, assign shared folder permissions. The following table shows shared folder permissions and the actions on shared folders allowed to users by the share permission.

Copyright © 2008 Microsoft Corporation.

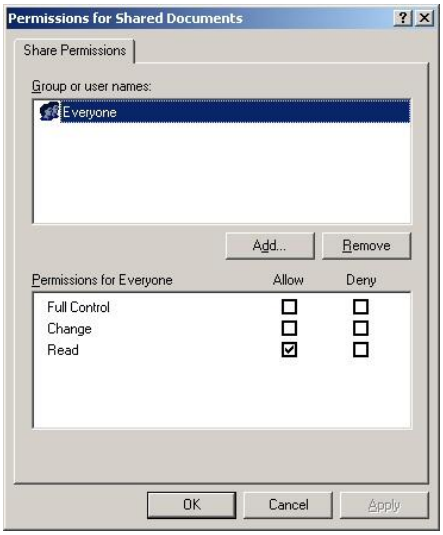
All rights reserved.

	Shared Folder Permission		
Actions Allowed by Share Permissions	**Full Control**	**Change**	**Read**
Viewing file names and subfolder names	✓	✓	✓
Traversing to subfolders	✓	✓	✓
Viewing data in files and running programs	✓	✓	✓
Adding files and subfolders to the shared folder	✓	✓	
Changing data in files	✓	✓	
Deleting subfolders and files	✓	✓	
Changing permissions (NTFS only)	✓		
Taking ownership (NTFS only)	✓		

Shared folder permissions can be set to allow or deny. Generally, it is best to allow permissions and to assign those permissions to a group rather than to individual users. Deny permissions should only be used when it is necessary to override permissions that are otherwise applied. In most cases, deny permissions should only be applied when it is necessary to deny permission to a specific user who belongs to a group to which has been given the permission. If a shared folder is set with deny permission to a user, the user will not have that permission. For example, to deny all access to a shared folder, deny the Full Control permission.

Default Share Permissions

Prior to the introduction of Windows Server 2003, all newly created share folders were automatically assigned the **Full Control** permissions for the group Everyone by default. This permission setting allowed **Full Control** share access to anyone that could reach the share on the network. To provide stronger security of shared resources and ensure that administrators take the time to implement proper share permissions, both Windows XP Professional with SP1 or higher and Windows Server 2003 change the default share permissions to grant only the **Read** permission to the Everyone group.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

The default permissions must be modified to **Full Control** or to add the **Change** permission if users will be required to add, delete, or modify objects in the share. Additionally, it is best to remove share permissions for the group Everyone and set permissions for explicit user or group accounts instead.

How Shared Folder Permissions are Applied

Applying shared permissions to user accounts and groups affects access to a shared folder. Denying permission takes precedence over the permissions that are allowed. The following list describes the effects of applying permissions.

- **Multiple Permissions Combine:** A user can be a member of multiple groups, each with different permissions that provide different levels of access to a shared folder. When permission is assigned to a user for a shared folder, and that user is a member of a group that is assigned a different permission, the user's effective permissions are the combination of the user and group permissions. For example, if a user has Read permission and is a member of a group with Change permission, the user's effective permission is Change, which includes Read.
- **Denying Permissions Overrides Other Permissions:** Denied permissions take precedence over any permissions that are otherwise allowed for user accounts and groups. If a user is denied permission to a shared folder using the **Permissions for <*share name*>** interface, the user will not have that permission, even if allowed the permission for a group of which the user is a member.
- **NTFS Permissions Are Required on NTFS Volumes:** Shared folder permissions are sufficient to gain access to files and folders on a FAT volume but not on an NTFS volume. On a FAT volume, users can gain access to a shared folder for which they have permissions, as well as all of the folder's contents. When users gain access to a shared folder on an NTFS volume, they need the shared folder permission and also the appropriate NTFS permissions for each file and folder to which they gain access.
- **Copied or Moved Shared Folders Are No Longer Shared:** When a shared folder is copied, the original shared folder is still shared, but the copy is not shared. When a shared folder is moved, it is no longer shared.

Guidelines for Shared Folder Permissions

The following list provides some general guidelines for managing shared folders and assigning shared folder permissions:

- Determine which groups need access to each resource and the level of access that they require. Document the groups and their permissions for each resource.
- Assign permissions to groups instead of user accounts to simplify access administration.
- Assign to a resource the most restrictive permissions that still allow users to perform required tasks. For example, if users need only to read information in a folder, and they will never delete or create files, assign the Read permission.
- Organize resources so that folders with the same security requirements are located within a common parent folder. For example, if users require Read permission for several application folders, store the application folders within the same parent folder. Then share this folder instead of sharing each individual application folder.
- Use intuitive share names so that users can easily recognize and locate resources. For example, for the Application folder, use Apps for the share name. Also use share names that all client operating systems can use.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Microsoft Windows Server 2003 provides 8.3-character equivalent names, but the resulting names might not be intuitive to users. For example, a Windows Server 2003 folder named Accountants Database would appear as Account~1 on networked systems that cannot read long file names.

Sharing Folders

Share resources with others by sharing the folders containing those resources. To share a folder, a user must be a member of one of several groups, depending on the role of the computer where the shared folder resides. When a folder is shared, access to the folder can be controlled by placing a limit on the number of users who can simultaneously access it, and access to the folder and its contents can also be controlled by assigning permissions to selected users and groups. Which groups can share folders and on which machines they can share them depends on whether it is a workgroup or a domain and the type of computer on which the shared folders reside:

- In a Windows Server 2003 domain, the Administrators and Server Operators groups can share folders residing on any machines in the domain. The Power Users group is a local group and can share folders residing only on the Windows Server 2003 stand-alone server or computer running Windows XP Professional where the group is located.
- In a Windows workgroup, the Administrators and Power Users groups can share folders on Windows Server 2003 or a computer running Windows XP Professional on which the group exists.

If the folder to be shared resides on an NTFS volume, users must also have at least the Read permission for that folder to be able to share it.

Administrative Shared Folders

Windows Server 2003 automatically shares folders for administrative purposes. These shares are appended with a dollar sign ($), which hides the shared folder from users who browse the computer through the network. The root of each volume, the system root folder, and the location of the printer drivers are all hidden shared folders. The following table describes the purpose of the administrative shared folders that Windows Server 2003 automatically provides.

Share	Purpose
C$, D$, E$, and so on	The root of each volume on a hard disk is automatically shared, and the share name is the drive letter appended with a dollar sign ($). Connecting to this folder, allows access to the entire volume. Use the administrative shares to remotely connect to the computer to perform administrative tasks. Windows Server 2003 assigns the Full Control permission to the Administrators group.
ADMIN$	The system root folder, which is C:\WINDOWS by default, is shared as Admin$. Administrators can gain access to this shared folder to administer Windows 2000 without knowing in which folder it is installed. Only members of the Administrators group have access to this share. Windows 2000 assigns the Full Control permission to the Administrators group.
IPC$	Interprocess communication share.
NETLOGON	A resource that is used on Domain Controllers. It is used when processing domain logon requests.
Print$	When the first shared printer is installed, the systemroot\ System32\Spool\Drivers folder is shared as Print$. This folder provides access to printer driver files for clients. Only members of the Administrators, Server Operators, and Print Operators groups have the Full Control permission. The Everyone group has the Read permission.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

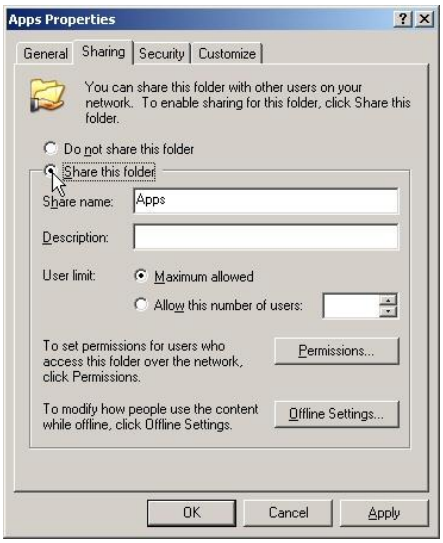
Share	Purpose
SYSVOL	A resource that is used on Domain Controllers. The system volume, is a collection of folders, file system reparse points, and Group Policy settings that are replicated by the File Replication Service (FRS). Replication distributes a consistent copy of Group Policy settings and scripts among Domain Controllers in a domain. Member computers and Domain Controllers access the contents of the SYSVOL tree through two shared folders, SYSVOL and NETLOGON.

Hidden shared folders are not limited to those that the system automatically creates. Additional folders can be shared and a dollar sign can be appended to the end of the share name. Then only users who know the folder name can gain access to it if they also possess the proper permissions to it.

Sharing a Folder

When a folder is shared, it can be given a share name, comments can be provided to describe the folder and its content, limits to the number of users who have access to the folder can be set, permissions can be assigned, and the folder can be shared multiple times. A folder can be shared as follows:

1. Log on with a user account that is a member of a group that is able to share folders.
2. Right-click the folder that is to be shared, and then click **Sharing and Security…**. The folder's **Properties** interface will appear, showing the options of the **Sharing** tab. Select the **Share this folder** radio button.



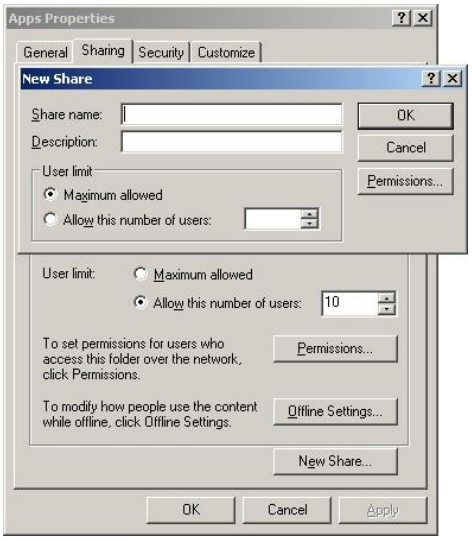
3. Configure the options shown in the table below to make the folder available as a share.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Option	Description
Share Name	The name that users from remote locations use to make a connection to the shared folder. A share name must be entered.
Comment	An optional description for the share name. The comment appears in addition to the share name when users at client computers browse the server for shared folders. This comment can be used to identify contents of the shared folder.
User Limit	The number of users who can concurrently connect to the shared folder. If Maximum allowed is selected as the user limit, Windows Server 2003 Server can support an unlimited number of connections, but the number of Client Access Licenses (CALs) that are purchased limits the connections.
Permissions	The shared folder permissions that apply only when the folder is accessed over the network. By default, the Everyone group is assigned **Read** permission for all new shared folders.
Offline Settings	The settings to configure offline access to this shared folder.

After the new share properties are applied, the share **Properties** interface will display a **New Share** button. This allows the creation of multiple network share names for the same folder.



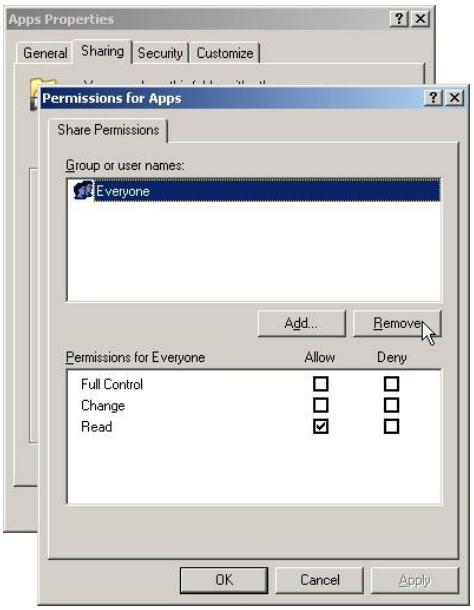
Assigning Shared Folder Permissions

After sharing a folder, the next step is to specify which users have access to the shared folder by assigning shared folder permissions to selected user accounts and groups. Assign permissions to user accounts and groups for a shared folder, as follows:

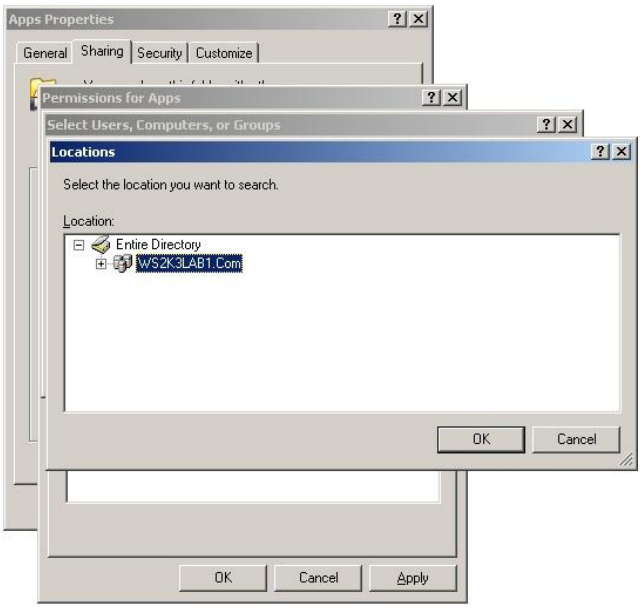
1. On the **Sharing** tab of the **Properties** interface of the shared folder, click **Permissions**.
2. In the **Permissions** interface, ensure that the Everyone group is selected and then click **Remove**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



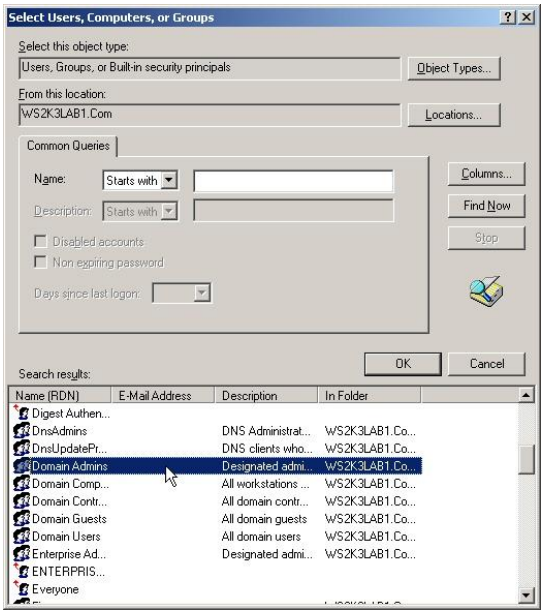
3. To set permissions for a new group or user, click **Add** to open the **Select User, Computer, or Group** (**Select Users or Groups** on a standalone system) interface. Enter the name of the user or group using the format *domainname\name* or click the **Advanced** button, then the **Find Now** button to select an account name from a list. To access account names from a domain, click the **Locations** button. There should now be a list that shows the local domain, trusted domains, and other resources that can be accessed. Select the local domain to view all the account names in the domain. Click **OK** to go back to the **Select Users, Computers, Or Groups** search tool interface.



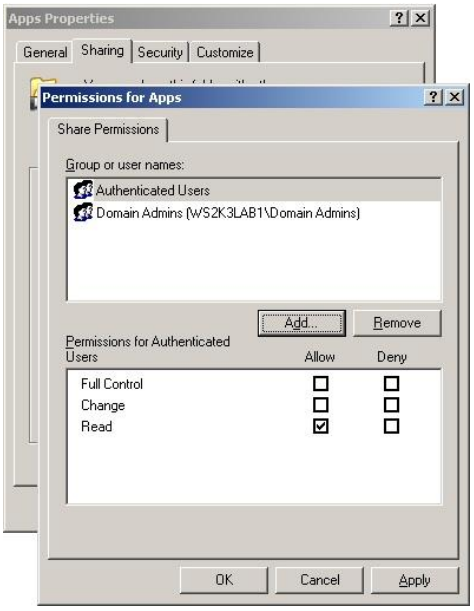
4. In the **Select Users, Computers, Or Groups** interface, click the user accounts and groups to which permissions are to be assigned and click **OK**. Repeat this step for all user accounts and groups to which permissions are to be assigned.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



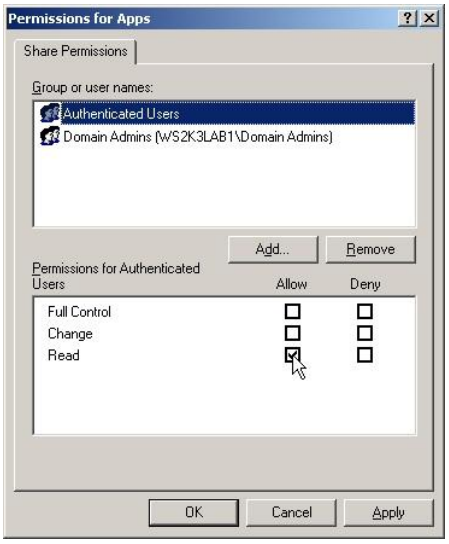
5. Once all accounts have been selected, click **OK** on the **Select Users, Computers, Or Groups** interface. The **Permissions** interface will show all the accounts that were added.

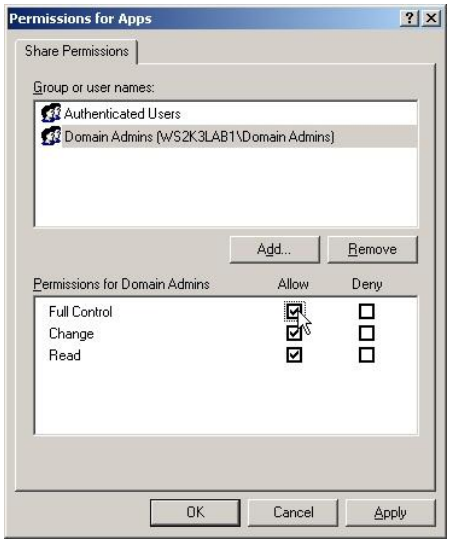


6. In the **Permissions** interface for the shared folder, select the user account or group, and then, under **Permissions for *<account name>***, select the **Allow** check box or the **Deny** check box to set the appropriate permissions for the user account or group.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



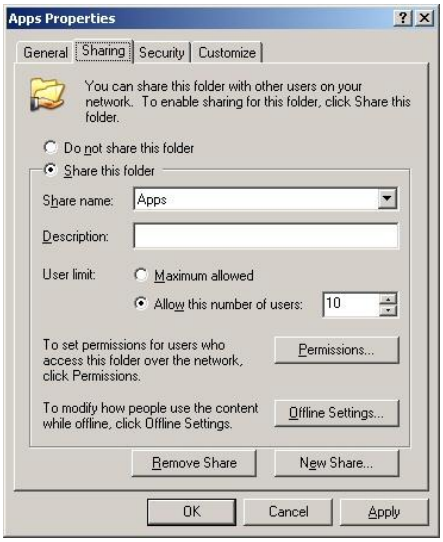


Modifying Shared Folders

Authorized users can modify shared folders, stop sharing a folder, modify the share name, and modify shared folder permissions.

Authorized users can modify a shared folder as follows:

1. Click the **Sharing** tab in the **Properties** interface of the shared folder.



2. To complete the appropriate task, use the steps in the table below.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

To	Do this
Stop sharing a folder	Click **Do not share this folder**.
Modify the share name	Click **Do not share this folder** to stop sharing the folder; click **Apply** to apply the change; click **Share this folder**, and then enter the new share name in the **Share name** box.
Modify shared folder permissions	Click **Permissions**. In the **Permissions** interface, click **Add** or **Remove**. In the **Name** interface, click the user account or group whose permissions are to be modified. Modify the permissions in the **Permissions: Allow** or **Deny** interface.
Share folder multiple times	Click **New Share** to share a folder with an additional shared folder name. Do so to consolidate multiple shared folders into one while allowing users to continue to use the same shared folder name that they used before consolidating the folders.
Remove a share name	Click **Remove Share**. This option appears only after the folder has been shared more than once.

Note: If sharing is disabled on a folder while a user has a file open, the user might lose data. If **Do not share this folder** is selected while a user has a connection to the shared folder, Windows Server 2003 displays a notification that a user has a connection to the shared folder.

Combining Shared Folder Permissions and NTFS Permissions

Folders can be shared to provide network users with access to resources. If using a FAT volume, the shared folder permissions are the only resource available to provide security for the folders that are shared and the folders and files they contain. If using an NTFS volume, NTFS permissions can be assigned to individual users and groups to better control access to the files and subfolders in the shared folders. When combining shared folder permissions and NTFS permissions, the more restrictive permission is always the overriding permission.

Shared folder permissions provide limited security for resources. The greatest flexibility can be gained by using NTFS permissions to control access to shared folders. Also, NTFS permissions apply whether the resource is accessed locally or over the network.

One strategy for providing access to resources on an NTFS volume is to share folders with the default shared folder permissions and then control access by assigning NTFS permissions. When a folder is shared on an NTFS volume both shared folder permissions and NTFS permissions combine to secure file resources.

When using shared folder permissions on an NTFS volume, the following rules apply:

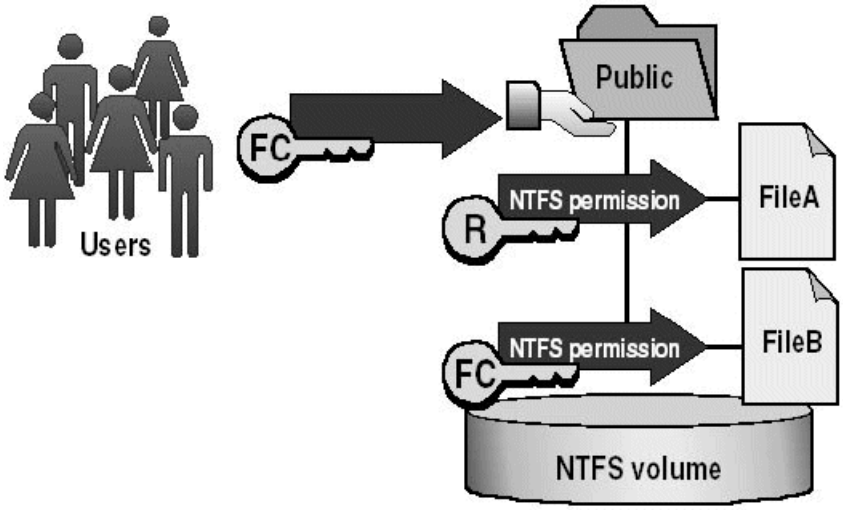
- NTFS permissions can be applied to files and subfolders in the shared folder. Different NTFS permissions can be applied to each file and subfolder that a shared folder contains.
- In addition to shared folder permissions, users must have NTFS permissions for the files and subfolders that shared folders contain to gain access to those files and subfolders. This is in contrast to FAT volumes where permissions for a shared folder are the only permissions protecting files and subfolders in the shared folder.
- When combining shared folder permissions and NTFS permissions, the more restrictive permission is always the overriding permission.

In the figure below, the Everyone group has the shared folder Full Control permission for the Public folder and the NTFS Read permission for File A. The Everyone group's effective permission for File A is Read

Copyright © 2008 Microsoft Corporation.

All rights reserved.

because Read is the more restrictive permission. The effective permission for File B is Full Control because both the shared folder permission and the NTFS permission allow this level of access.



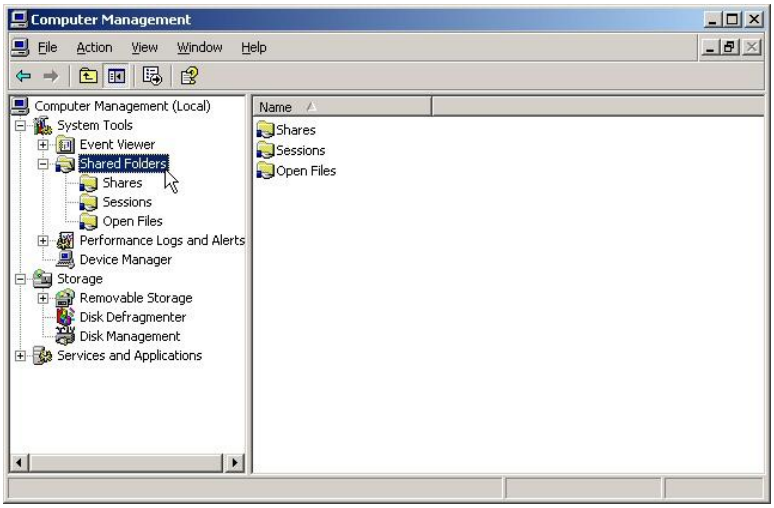
- NTFS permissions are required on NTFS volumes.
- Apply NTFS permissions to files and subfolders.
- The most restrictive permission is the effective permission.

Disconnecting a User or Users from a Share or Active Session

Authorized users can manage shares and disconnect active sessions from the **Shared Folders** object in the **Computer Management** GUI. For Windows Server 2003, members of the Administrators, Power Users, and Server Operators group can use the **Shared Folders** object. Note that disconnecting users who are using resources may result in loss of data. It is a good idea to warn connected users before disconnecting them.

Disconnect a user or group of users as follows:

1. Click **Start**, point to **Administrative Tools**, select **Computer Management**, and then double-click **Shared Folders**.

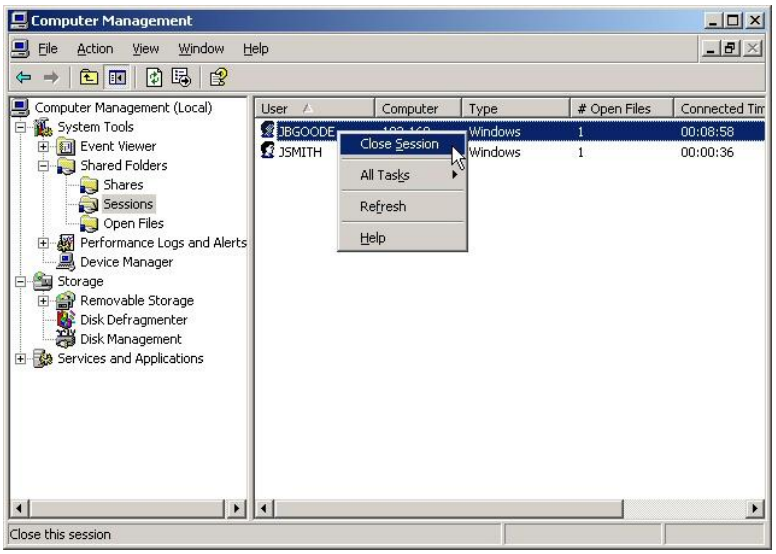


2. In the console tree, click **Sessions**. All active sessions, showing users accessing shared resources, will be displayed in the right-hand pane.

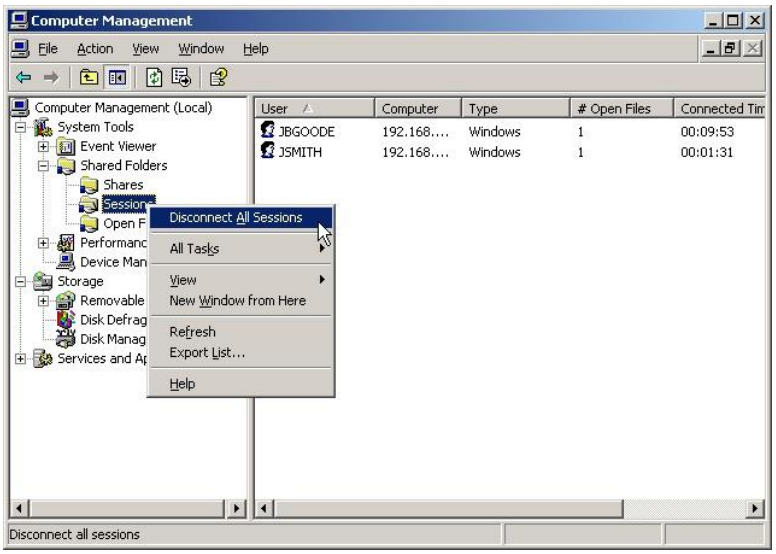
Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. To disconnect one user, right-click the user name and then select **Close Session**.



4. To disconnect all users, right-click **Sessions**, and then select **Disconnect All Sessions**.



Note: The procedures above will disconnect active sessions, but will not prevent further access to the shares. Although the users will be disconnected, this measure is only temporary because, as long as they are authorized access to the share, the users will be able to re-connect to them at any time. To fully deny access to a user, change the access permissions on the share.

Active Directory Object Permissions

In Active Directory, access control is administered at the object level by setting different levels of access, or permissions, to objects, such as Full Control, Write, Read, or No Access. Access control in Active Directory how different users can use Active Directory objects. By default, permissions on objects in Active Directory are set to the most secure setting. In controlling access to Active Directory objects, there are two things to consider: the permissions that a user is allowed to attach to the object and the ways in which these permissions can be attached in order to delegate administrative responsibility for Active Directory objects.

Copyright © 2008 Microsoft Corporation.

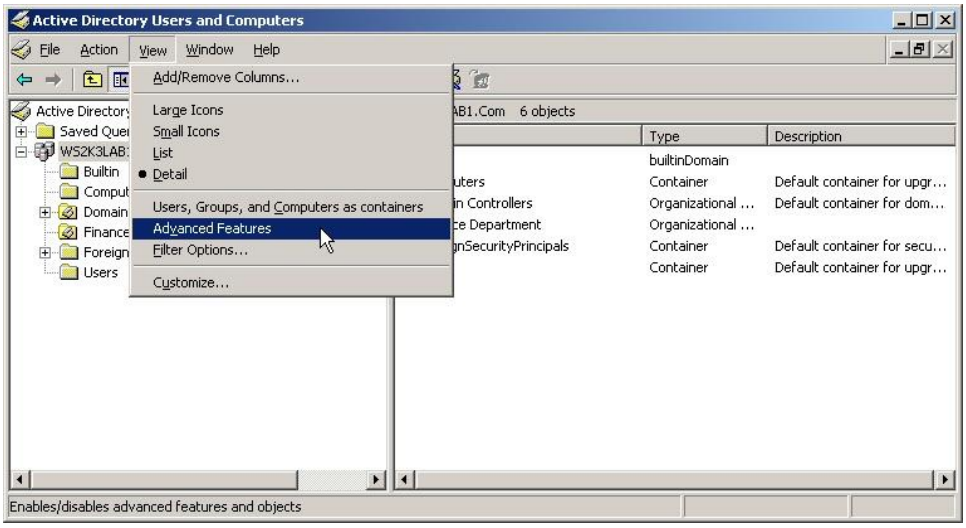
All rights reserved.

Active Directory objects can have the following permissions attached to them:

- Create Child (can be specific to the type of object or general for any object under the container)
- Delete Child (can be specific to the type of object or general for any object under the container)
- Read Property (can be specific to an individual property of the object or general for all attributes of the object)
- Write Property (can be specific to an individual property of the object or general for all attributes of the object)
- List Contents
- Write Self
- Delete Tree
- List Object
- Control Access (can be specific to an individual control operation or general for all control operations on the object)

Permissions can be set on a directory object using the following procedure:

1. Log on to the Domain Controller as an authorized administrator.
2. Open the **Active Directory Users and Computers** interface.
3. On the **View** menu, select **Advanced Features**.



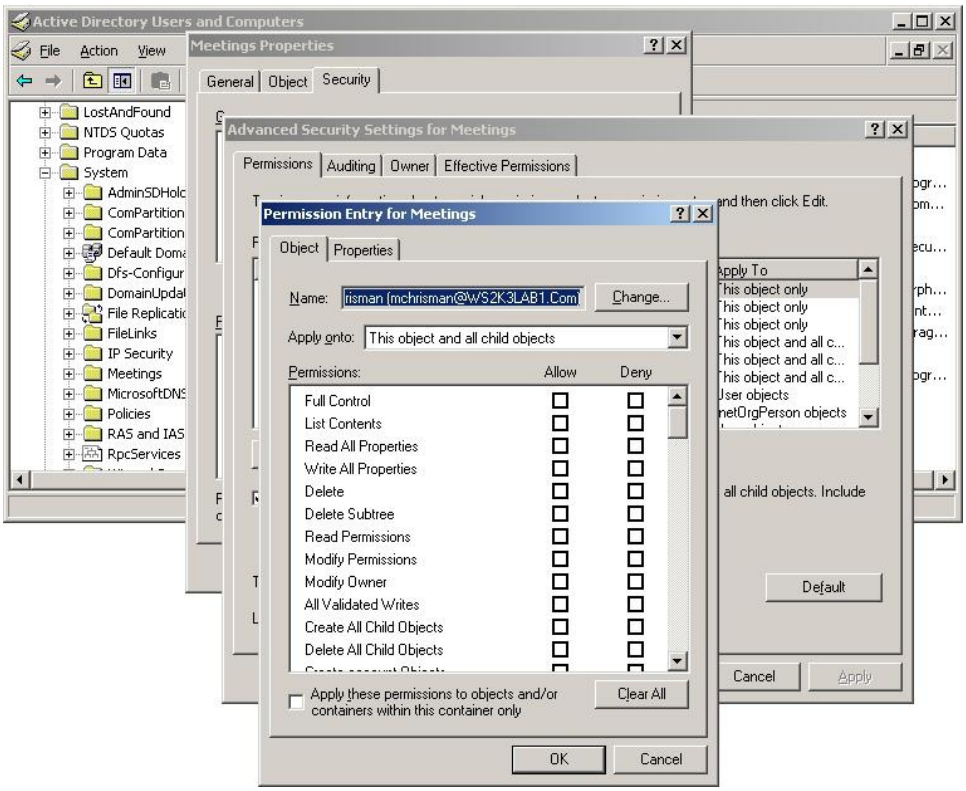
4. Locate the container for the object, right-click it, and then select **Properties**.
5. Click the **Security** tab, and click **Advanced**.
6. To add permissions for an account click the **Add** button. To edit existing permissions, select the account and click the **Edit** button. To remove existing permissions for an account, select the account and click the **Remove** button.
7. As an example, the **Add** button to open the **Select User, Computer, or Group** interface and add permissions for an account.
8. Enter the name of the user or group using the format *domainname\name* or click the **Advanced** button, then the **Find Now** button to select an account name from a list. To access account names from a domain, click the **Locations** button. There should now be a list that shows the local domain, trusted domains, and other resources that can be accessed. Select the local domain to view all the

Copyright © 2008 Microsoft Corporation.
All rights reserved.

account names in the domain. Click **OK** to go back to the **Select Users, Computers, Or Groups** search tool interface.

9. In the **Select Users, Computers, Or Groups** search tool interface, click the user account or group to which permissions are to be assigned and click **OK**. Click **OK** on the **Select Users, Computers, Or Groups** interface.

10. The **Permissions for <*container name*>** interface for the account will appear. The interface has two tabs—**Object** and **Properties**.



11. The **Object** tab allows an authorized administrator to specify access permissions to the object.

12. The **Properties** tab allows an authorized administrator to specify access permissions to the object properties.

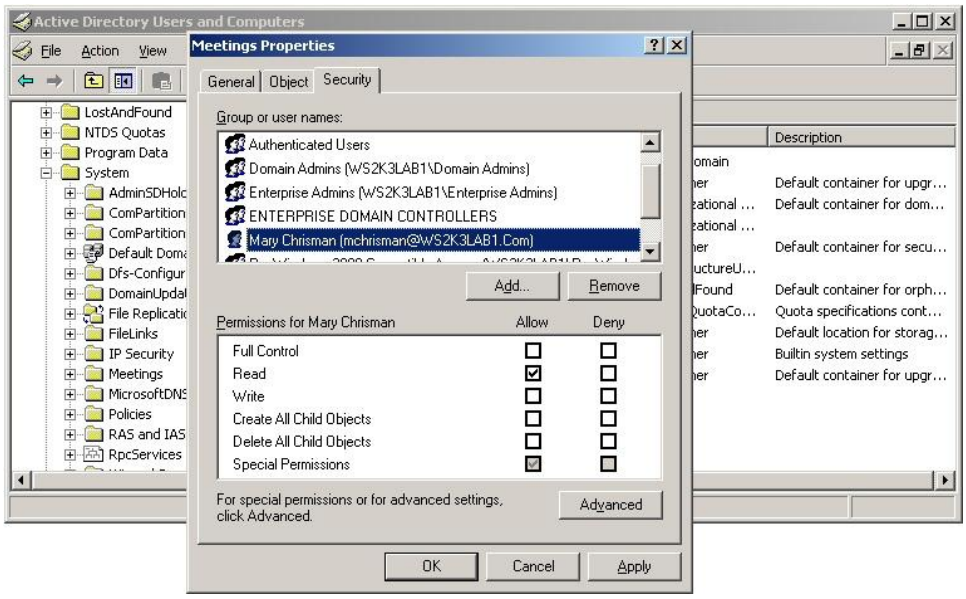
13. Click each tab that is to be modified, and select the check boxes for the permissions to be set.

14. Under **Permissions**, select the **Allow** check box or the **Deny** check box to set the appropriate permissions for the user account or group. Click **OK**.

15. Click OK on the **Advanced Security Settings for <*container name*>** interface. The new permissions will appear on the container **Properties** interface.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



16. Repeat the steps above for all user accounts or groups to which permissions are to be assigned.
17. When finished, click **OK** on the **Properties** interface.

Setting Printer Security Permissions and Printer Shares

When a printer is installed on a network, default permissions are assigned that allow all users to print, and allow select groups to manage the printer, the documents sent to it, or both. Because the printer is available to all users on the network, it might be necessary to limit access for some users by assigning specific printer permissions. For example, all non-administrative users in a department could be given the Print permission and all managers could be given the Print and Manage Documents permissions. In this way, all users and managers can print documents, but managers can also change the print status of any document sent to the printer.

Windows Server 2003 provides three levels of printing security permissions: **Print**, **Manage Printers**, and **Manage Documents**. When multiple permissions are assigned to a group of users through the printer **Properties** interface, the least restrictive permissions apply. However, when **Deny** is applied, it takes precedence over any permission. The table below provides a brief explanation of the types of tasks a user can perform at each permission level.

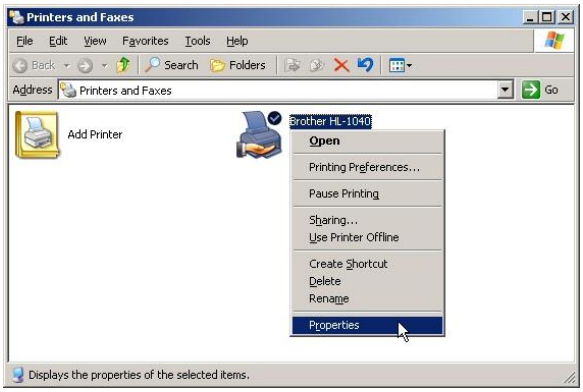
Copyright © 2008 Microsoft Corporation.

All rights reserved.

Permission	Description
Print	The user can connect to a printer and send documents to the printer. By default, the Print permission is assigned to all members of the Everyone group.
Manage Printers	The user can perform the tasks associated with the Print permission and has complete administrative control of the printer. The user can pause and restart the printer, change spooler settings, share a printer, adjust printer permissions, and change printer properties. By default, the Manage Printers permission is assigned to members of the Administrators and Power Users groups. By default, members of the Administrators and Power Users groups have full access, which means that the users are assigned the Print, Manage Documents, and Manage Printers permissions.
Manage Documents	The user can pause, resume, restart, and cancel documents submitted by all other users. The user cannot, however, send documents to the printer or control the status of the printer. By default, the Manage Documents permission is assigned to members of the Creator Owner group. When a user is assigned the Manage Documents permission, the user cannot access existing documents currently waiting to print. The permission will only apply to documents sent to the printer after the permission is assigned to the user.
Deny	Any or all of the preceding permissions are denied for the printer. When access is denied, the user cannot use or manage the printer, manipulate documents sent to the printer, or adjust any of the permissions.

Use the following procedures to set or remove permissions for a printer:

1. Click **Start** and select **Printers and Faxes**.
2. Right-click the printer object for which permissions are to be set, select **Properties**. The printer **Properties** interface will appear.

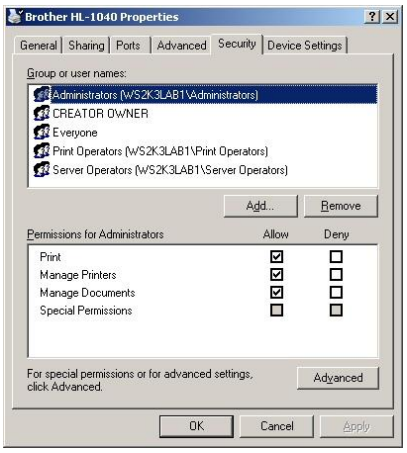


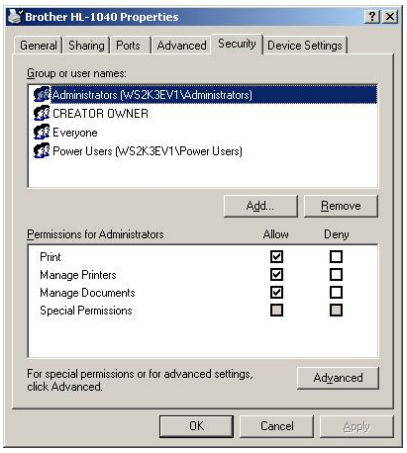
3. Click the **Security** tab and do one of the following:

- To change or remove permissions from an existing user or group, select the name of the user or group.

Copyright © 2008 Microsoft Corporation.

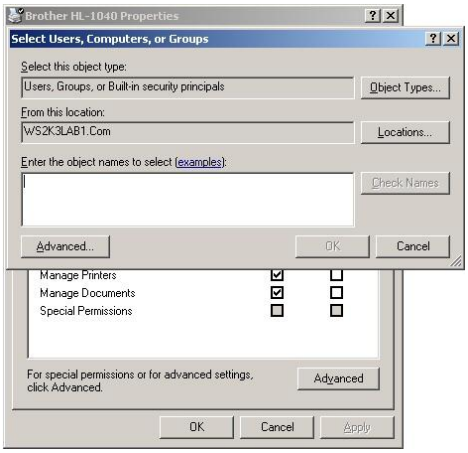
All rights reserved.





Note: As shown above, for network printers managed from a Windows Server 2003 print server, the default permissions are set for Administrators, CREATOR OWNER, Everyone, Print Operators, and Server Operators.

- To set permissions for a new group or user, click **Add** to open the **Select User, Computer, or Group** (**Select Users or Groups** on a standalone system) interface. Enter the name of the user or group using the format *domainname\name* or click the **Advanced** button, then the **Find Now** button to select an account name from a list. To access account names from a domain, click the **Locations** button. There should now be a list that shows the current machine, the local domain, trusted domains, and other resources that can be accessed. Select the local domain to view all the account names in the domain. Click **OK** to go back to the **Select Users, Computers, Or Groups** interface. Click **OK** to see the permission in the **Properties** interface.



- In **Permissions for <*account name*>**, click **Allow** or **Deny** for each permission that is to be allowed or denied for a selected user or group. Or, to remove the user or group from the permissions list, select the user or group and click **Remove**.
- After making all necessary permission assignments, click the **Apply** and then click **OK** on the printer **Properties** interface.

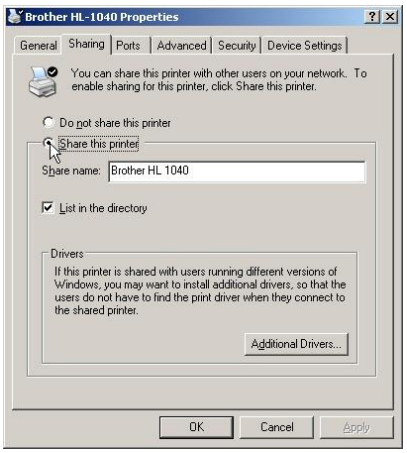
Note: To change device settings, a user must have the **Manage Printers** permission. To view or change the underlying permissions that make up **Print**, **Manage Printers**, and **Manage Documents**, click the **Advanced** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

During the printer installation process, a decision is made to share or not share the printer. Use the following procedures to change the sharing criteria for a printer after it has been installed (a printer must be shared in order for the permission settings to affect the users and groups listed):

1. Click **Start**, point to **Printers and Faxes**.
2. Right-click the printer to be shared, and select the **Sharing** option from the menu.
3. To share the printer, select the **Shared as** radio button, and then type a name for the shared printer. To disable sharing of the printer, select the **Do not share the printer** radio button.



4. If the printer is to be shared with users on different hardware or different operating systems, click **Additional Drivers**. Click the environment and operating system for the other computers, and then click **OK** to install the additional drivers.
5. If logged on to a Windows Server 2003 domain, the printer can be made available to other users in the domain by checking **List in the directory** to publish the printer in the Directory.
6. Click **OK**.

Delegating Administrative Control

An authorized administrator can define delegation of responsibility to create new users or groups at the level of the organizational unit, or container, where the accounts are created. Group administrators for one organizational unit do not necessarily have the ability to create and manage accounts for another organizational unit within a domain. However, policy settings that are domain wide and permissions that are defined at higher levels in the directory tree can apply throughout the tree by using inheritance of permissions.

There are three ways to define the delegation of administration responsibilities:

- Delegate permissions to change properties on a particular container.
- Delegate permissions to create and delete objects of a specific type under an organizational unit, such as users, groups, or printers.
- Delegate permissions to update specific properties on objects of a specific type under an organizational unit. For example, the right to set a password on a User object can be delegated.

An authorized administrator can delegate administration of particular resources to a specific individual or group, eliminating the need for multiple administrators to have authority over an entire domain or site. With appropriate delegation, the user or group who has been granted the appropriate permissions can, in turn, delegate administration of a subset of their accounts and resources.

Copyright © 2008 Microsoft Corporation.

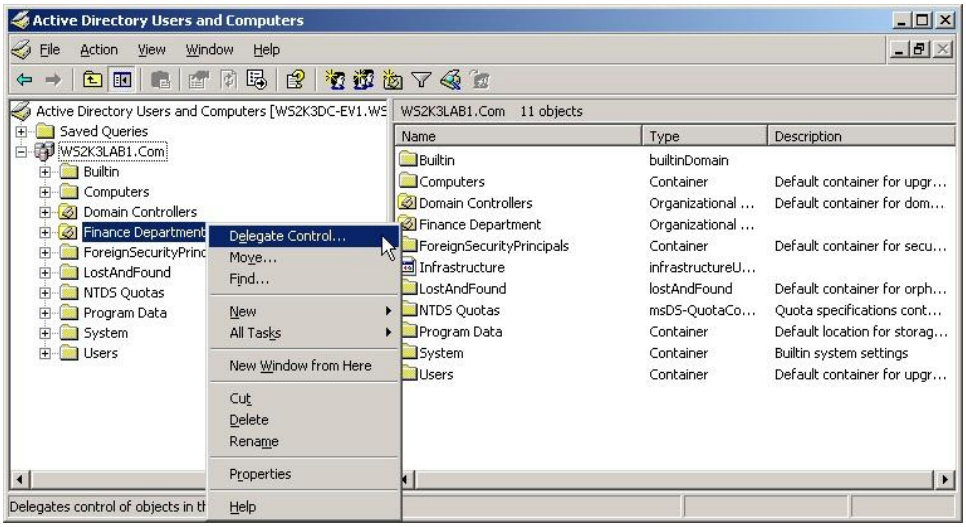
All rights reserved.

The administrator can configure the scope of delegated administrative responsibility in many different ways. Although authorized administrators can generally grant permissions at the organizational unit level by applying inheritance, they can also delegate administration for an entire domain within a forest.

An authorized administrator can delegate administration of a domain or organizational unit by using the **Delegation of Control Wizard** available in **Active Directory Users and Computers**:

Note: For more details on delegating administrative control in Active Directory, see *Best Practices for Delegating Active Directory* at http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3&displaylang=en

1. Log on to the Domain Controller as an authorized administrator.
2. Open the **Active Directory Users and Computers** interface.
3. Locate the container for the object, right-click it and then click **Delegate Control…**.

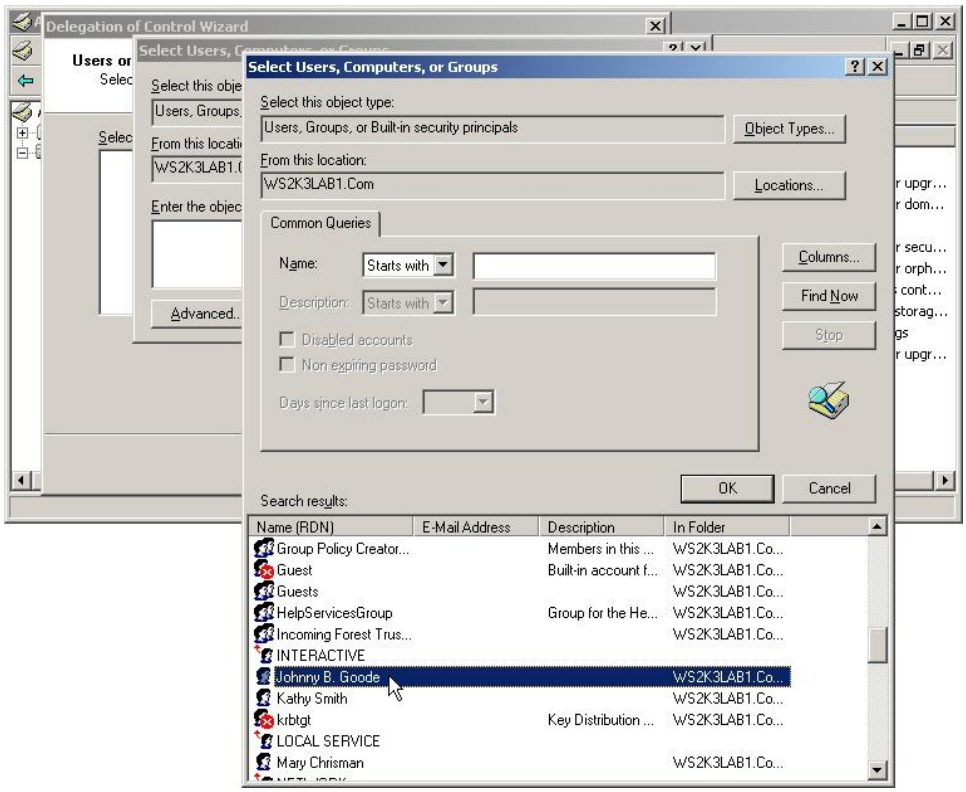


4. The **Delegation of Control Wizard** appears, click **Next**.

5. A Wizard window appears for selection of **Users or Groups**, click the **Add** button. Select an account using the **Select Users, Computers, or Groups** interfaces.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



6. When the desired accounts have been added to the **Selected Users and groups** list, click **Next**.

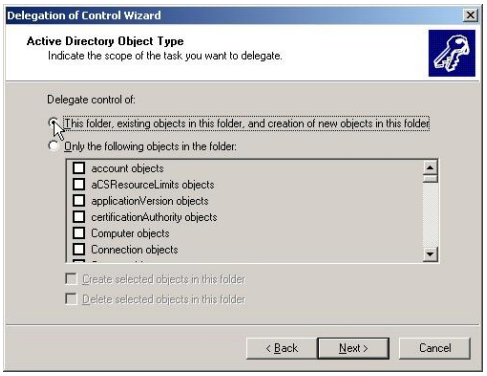
7. The next Wizard view allows the options of delegating common tasks or creating a custom task to delegate.

   - Click the **Delegate the following common tasks** radio button and select tasks from the list by checking the appropriate boxes; or

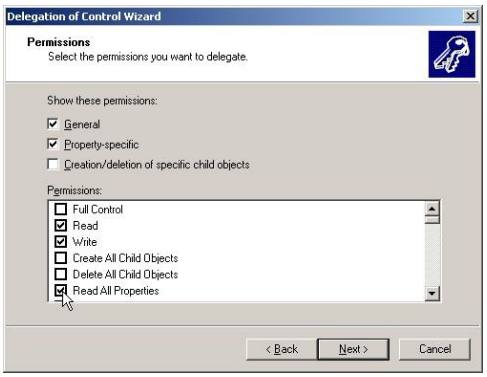
Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Click the **Create a custom task to delegate** radio button and click **Next**. The next Wizard view provides two options for defining the scope of delegation. The first option, **This folder, existing objects in folder, and creation of new objects in this folder**, allows delegation of full control. The second option, **Only the following objects in the folder**, opens a selection window that allows administrators to specify the level of control they want to delegate.



- Make a selection and click **Next**. The next window allows for the specifications of the permissions to delegate. Select the permissions to delegate and click **Next.**



8. A completion window will appear describing the selections. Click the **Finish** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Content Indexing Service

Indexing Service extracts the information from documents stored on a computer and organizes it in a way that provides rapid access to files through flexible querying language. This makes it quicker and easier to find information using the Search function in Microsoft Windows Server 2003. An end user of Indexing Service usually accesses the components of Indexing Service through the Microsoft Management Console (MMC) or the **Start**, **Search for Files**, or **Folder** dialog box of Windows Server 2003. Through a process called indexing, Indexing Service uses a document filter to read through a document and extract text and properties to store in the indexer.

Document properties represent the characteristics of the document, such as date created, author name, and size. Property values are the specific information for a particular document. Some property values are set automatically by the program that creates the document; others are entered by the user.

All properties and property values are indexed with the document contents and can be searched. Most properties can also be displayed in the list of search results. However, some properties, such as those in the Meta tags of HTML documents, must be stored in the property cache when the document is indexed. Otherwise, Indexing Service is unable to retrieve them for display in the results of a search. Administrators can specify which properties to save in the property cache if the default selection does not meet current needs.

Index Service extracts and stores information on local fixed disks and shared network drives. Information on removable drives is not indexed. During installation, Indexing Service creates a default catalog called System. Catalogs can be added and removed at any time. Pre-existing catalogs can also be configured. If Internet Information Services (IIS) is running on the computer, Indexing Service also creates a catalog called the Web catalog.

After the index is created users can query the index for files that contain key words, phrases, or properties. This is done using the Search feature on the Start menu in Windows. Indexing Service is designed to run continuously and requires little maintenance. After it is set up, all operations are automatic, including index creation, index updating, and crash recovery if there is a power failure.

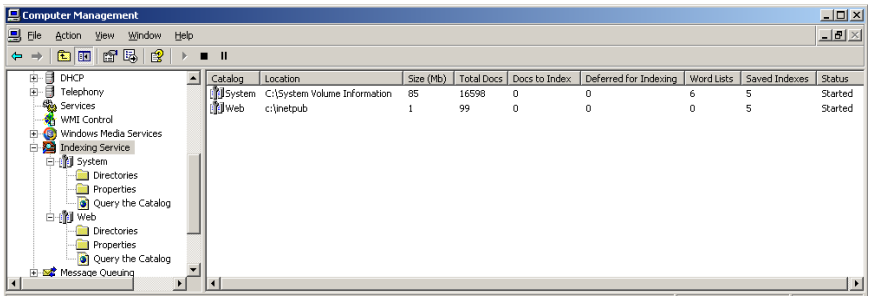
Accessing Indexing Service

To access Indexing Service:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand the **Services and Applications** container and then expand **Indexing Service**. Select **Indexing Service**. The details pane for Indexing Service displays catalog status information.

Copyright © 2008 Microsoft Corporation.

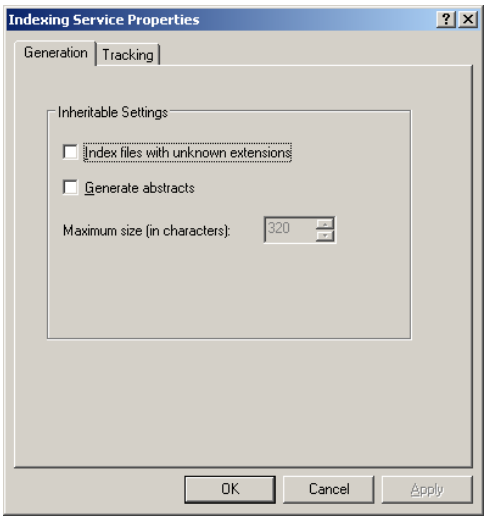
All rights reserved.



Configuring Indexing Service Properties

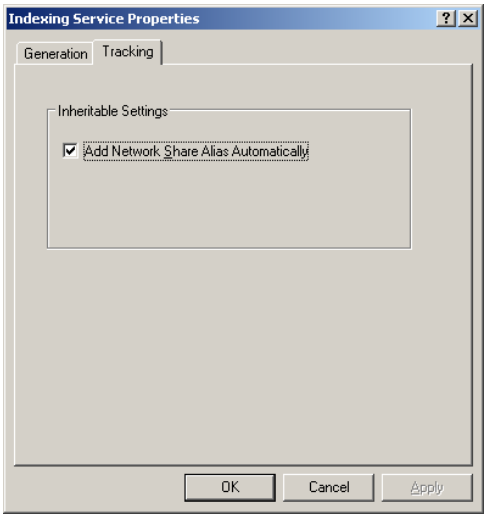
To configure Indexing Service:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand the **Services and Applications** container and then expand **Indexing Service**. Select **Indexing Service**.
4. On the **Action** menu, select **Properties**.
5. In the **Indexing Service Properties** interface, select the **Generation** tab, and then select the appropriate check boxes as follows:
   - To index documents with unknown extensions (those not having filters installed), select the **Index files with unknown extensions** check box. Indexing Service extracts whatever content and properties it can from the documents.
   - To produce abstracts of documents to display in the results list, select the check box for **Generate abstracts**. In the Maximum size box, type the maximum number of characters for the abstracts.



6. Click the **Tracking** tab.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

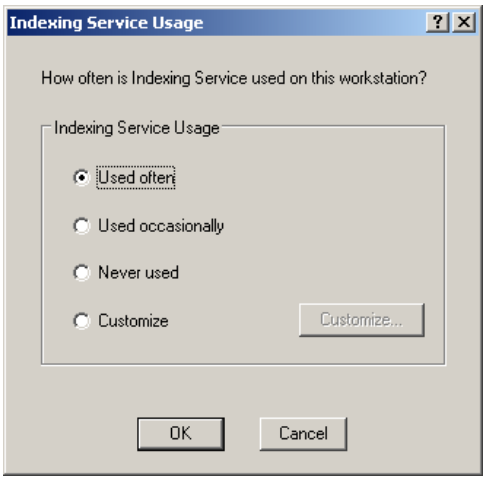


7. If it is desired to have Indexing Service use the share name of a shared folder as the alias for that folder, select the check box for **Add Network Share Alias Automatically**.
8. Click **OK**.
9. Stop the Indexing Service by right-clicking the **Indexing Service** container in the console tree, and selecting **Stop**.
10. Restart the Indexing Service by right-clicking the **Indexing Service** container in the console tree, and selecting **Start**.

Configuring Indexing Service Usage

To tune the performance of Indexing Service:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand the **Services and Applications** container.
4. In the console tree, right-click **Indexing Service**, point to **All Tasks**, and select **Tune Performance**. The Indexing Service Usage interface is displayed.

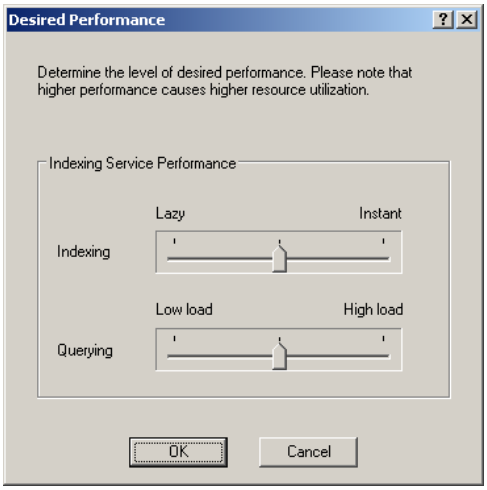


5. Select the appropriate radio button, according to the following:

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- **Used often** specifies that Indexing Service is used often enough on this computer to require better than average performance.
- **Used occasionally** specifies that Indexing Service is not used often enough on this computer to require better than average performance
- **Never used** specifies that Indexing Service is never used on this computer. The service will be turned off.
- **Customize** enables the Customize button to allow configuration of personalized performance tuning settings.

6. Clicking on the **Customize** button opens the Desired Performance interface.



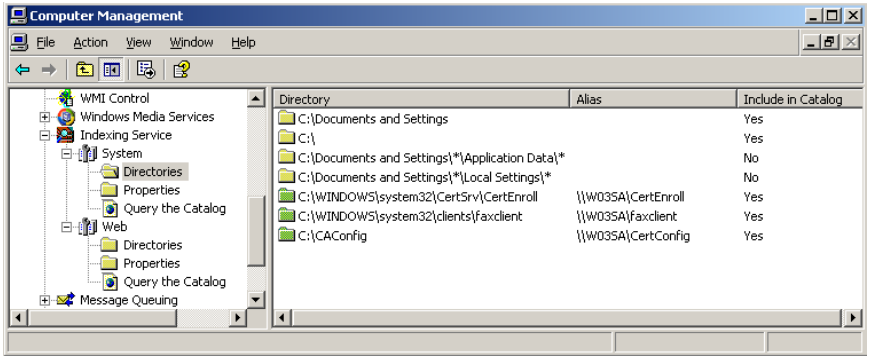
7. To configure Indexing Service performance, specify the level of desired performance as follows:
   - In the **Desired Performance** dialog box, move the **Indexing** slider to **Lazy** for less immediate indexing or to **Instant** for immediate indexing of new and changed documents. Lazy indexing uses fewer resources; Instant indexing uses as much of the computer's resources as it can.
   - Move the **Querying** slider to **Low load** to process only a few queries at a time or to **High load** if it is expected to process many queries at a time. Low load uses fewer resources; high load uses more.
8. Click **OK** twice and close the Computer Management interface.

Controlling System Catalog Directories

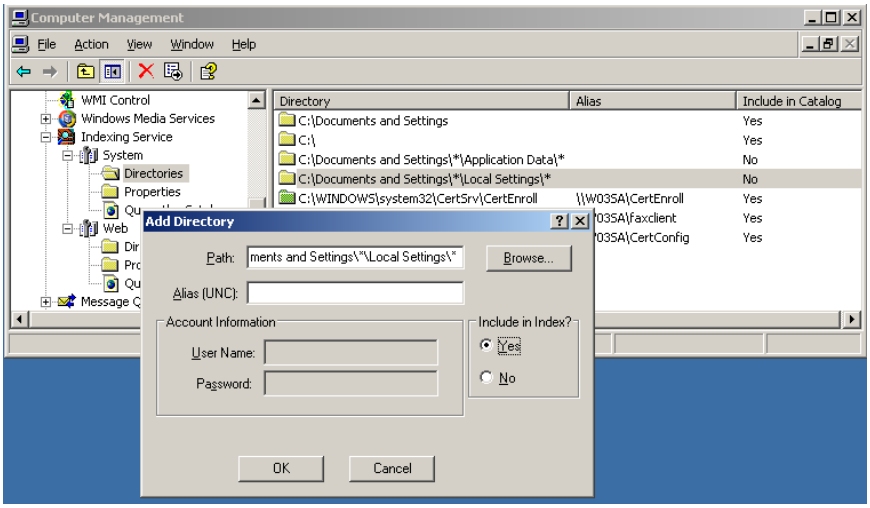
To control system catalog directories:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand the **Services and Applications** container and then expand **Indexing Service**.
4. Select **Directories**. A list of local folders opens in the details pane, displaying each folder name, alias (if any), and whether or not that folder is included in the catalog. All content in folders marked **Yes** are indexed in the Search function. As a security feature, administrators can control searchable content by designating **Yes** or **No** in the catalog. To include this folder in the index, select the **Yes** radio button, and then click **OK**.

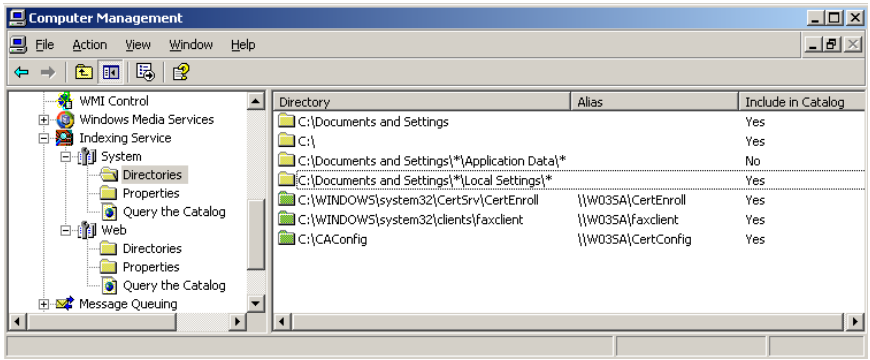
Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. To include or exclude a folder in the catalog, double-click the folder. The **Add Directory** dialog box opens. For example, the Documents and Setting*\Local Settings* folder is set to **No**. To set the folder to **Yes**, double-click the folder.



6. The **Local Settings** folder is now included in the catalog and will be indexed the next time a scan runs.



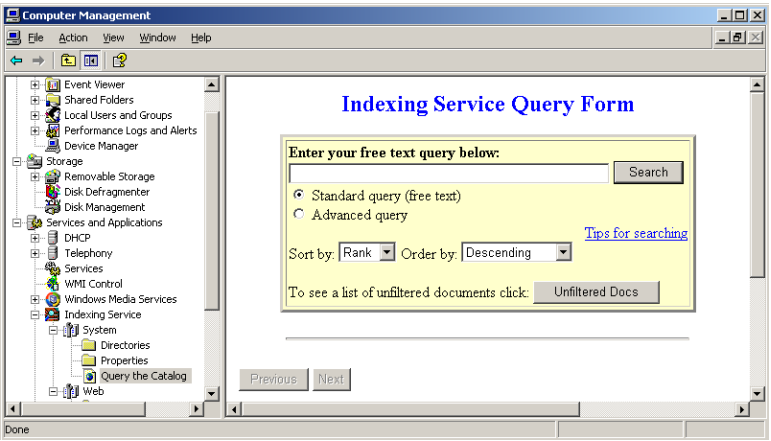
Querying the System Catalog

To display the Indexing Service Query Form in the details pane of the console:

Note: The Web catalog is available only on computers running IIS and can be managed using the same procedures shown in the example below.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Computer Management**.
3. Expand the **Services and Applications** container and then expand **Indexing Service**.
4. Select **Query the Catalog**.

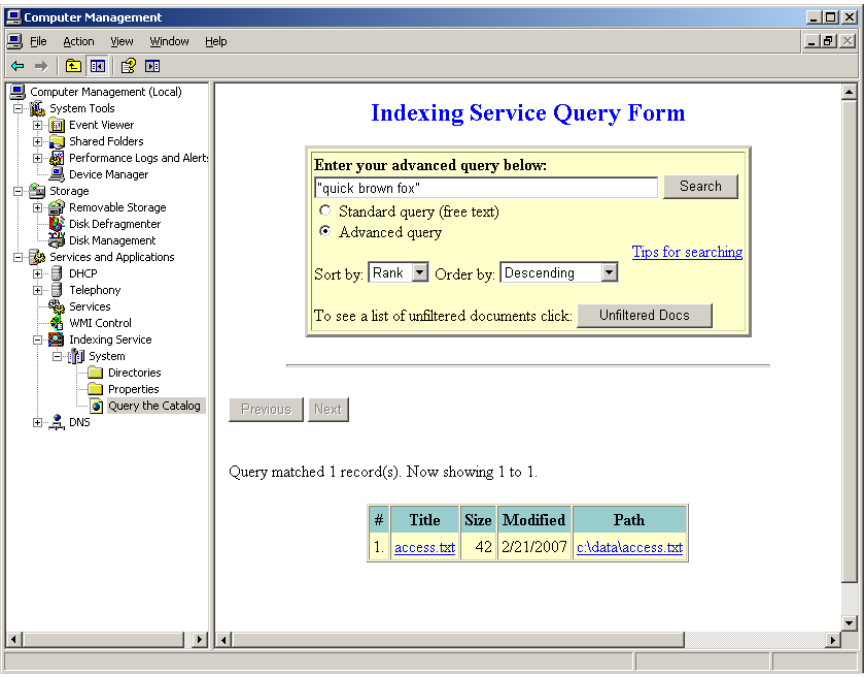


5. Type the query in the field provided, adhering to the following rules:
   - Queries are not case-sensitive.
   - Search for any word except words that are on the exception list. Exception words are ignored during the search. Exception words (such as articles, prepositions, pronouns) are not indexed. To view the Exception-word list, select **Help** from the **Action** menu on the main menu bar, and expand **Indexing Service** on the **Contents** tab. Under **Advanced Topics**, expand **Understanding Indexing Service**, expand **Indexing Overview**, and then click **Exception-word list**.
   - Enclose special characters within quotation marks.
   - Date and time values adhere to the following format: *yyyy/mm/dd hh:mm:ss* or *yyyy-mm-dd hh:mm:ss*

   Note: To view general rules for queries, select **Help** from the **Action** menu on the main menu bar, and expand **Indexing Service** on the **Contents** tab. Under **Advanced Topics**, expand **Indexing Service Query Language**, expand **Queries and Query Language**, and then click **General rules for queries**.

6. Select the **Standard query (free text)** or **Advanced query** radio button.
7. Use the **Sort by** drop-down list box and **Order by** drop-down list box to select how the search results should be displayed.
8. Click **Search**. The search results are displayed.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



Scheduled Tasks

In Microsoft Windows Server 2003, the Scheduled Tasks interface is used to display, create, delete, or modify scheduled tasks. Using Scheduled Tasks, any script, program, or document can be scheduled to run at a time that is most convenient. Additional items Scheduled Tasks can perform include:

- Schedule a task to run daily, weekly, monthly, or at certain times (such as system startup)
- Modify or delete a scheduled task
- Stop a scheduled task that is running
- Disable all scheduled tasks

When a scheduled task is created, an auditable object (in the form of a *.job file) is created that is accessible to other processes and, in some cases, other users. The task creator can assign object access permissions to users and security groups.

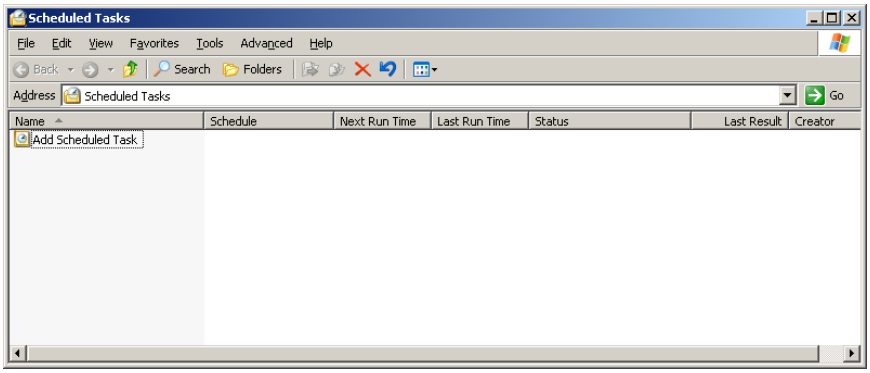
Adding and managing Scheduled Tasks

To use Scheduled Tasks, local user or administrative privileges are needed on the computer and the Task Scheduler Service must be running and configured to **Log On as the Local System Account**. No special configuration is required to use Scheduled Tasks; however, prior to using Scheduled Tasks, the system date and time on the computer should be confirmed accurate. Scheduled Tasks relies on this information to run scheduled tasks. To verify or change the date or time, double-click the time indicator in the system tray, or access the Date and Time applet with the Control Panel. When Scheduled Tasks is run initially, by default, no tasks appear in the task list.

Note: Non-administrative user accounts are restricted from running applications via Scheduled Tasks by the applications own access control and privilege requirements.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



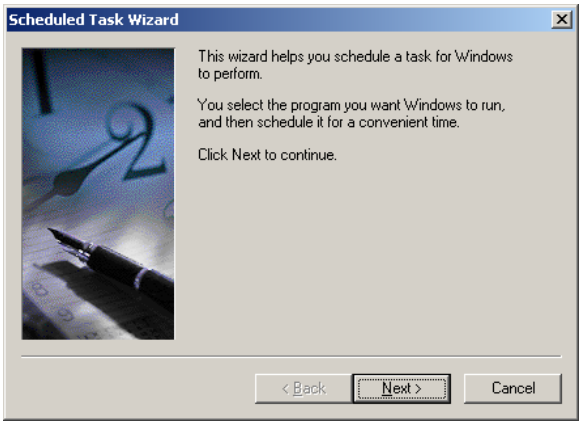
To add a scheduled task to the Scheduled Tasks folder, use the **Add Scheduled Task** icon to run the Scheduled Tasks Wizard. Scheduled Tasks provides user interfaces for the following functions, which are described in detail in this design specification.

- Add a scheduled task
- Modify a scheduled task
- Remove a scheduled task
- Stop or start a scheduled task
- Disable all scheduled tasks
- View a log of past scheduled tasks
- Receive notification of missed tasks
- View Scheduled Tasks on a remote computer

Scheduling a regularly occurring task

Tasks can be scheduled to run at a defined interval – daily, weekly, or monthly. In the following example procedure, the administrator configures a task that runs Internet Explorer at a particular time each day.

1. Click **Start**, point to **Control Panel**, point to **Scheduled Tasks**, and then select **Add Scheduled Task**. The Scheduled Task Wizard is displayed. Click **Next**.



2. Choose a program from the list by clicking it. In this example, Internet Explorer is the program selected. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. Type a name for the task, then select the radio button for Daily. Click **Next**.

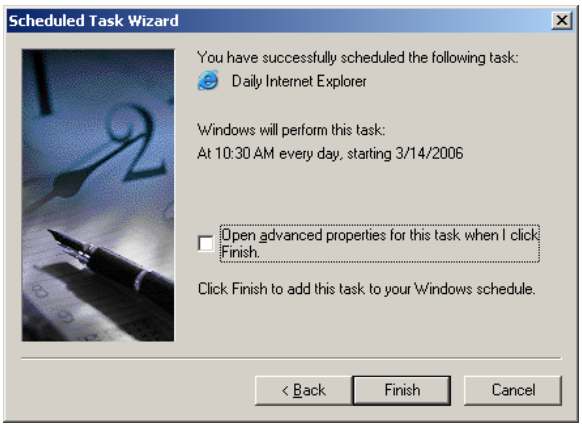
4. Select a **Start time** (for test purposes, choose a time that is later than the current time), and click **Next**.

5. Type the user name to run the task under. Use the format <DomainName>\<UserName>. Enter the user's password twice in the appropriate text boxes, and click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

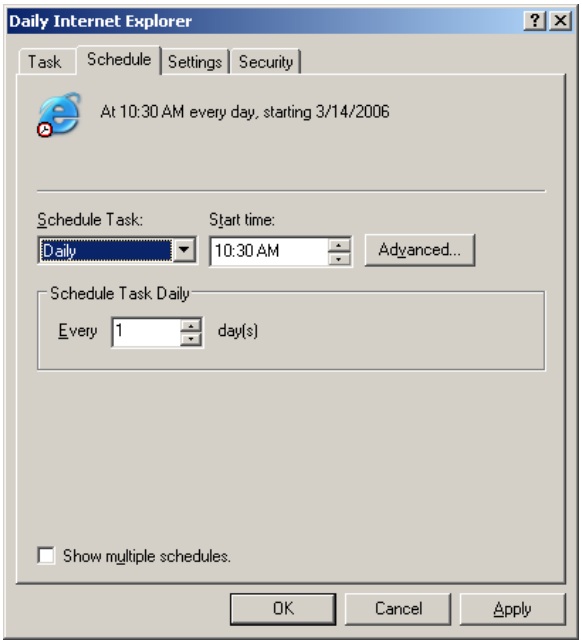
Note: In the evaluated configuration, user passwords are to remain private and administrators can therefore only schedule tasks for their own accounts. When an administrator uses the Add Scheduled Task Wizard to schedule a task to run under a particular user name and password, that user is automatically assigned the "Log on as a batch job" right. When the scheduled time arrives, the Task Scheduler Service logs the user on as a batch job rather than as an interactive user, and the task runs in the user's security context.

6. To exit the Scheduled Task Wizard, click **Finish**. Or, if it is desired to configure advanced settings for the task, such as security permissions for accessing the scheduled task object, select the **Open advanced properties for this task when I click Finish** check box on the final page of the wizard, and then click **Finish**.

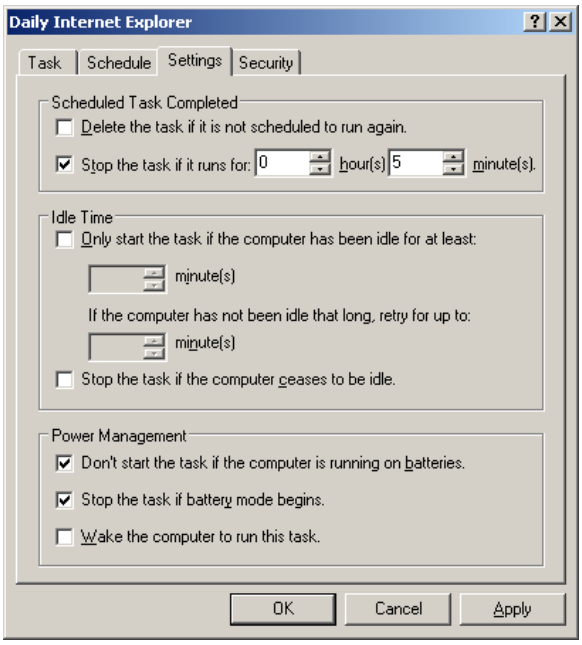


7. Click the **Schedule** tab to verify the schedule is correct.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

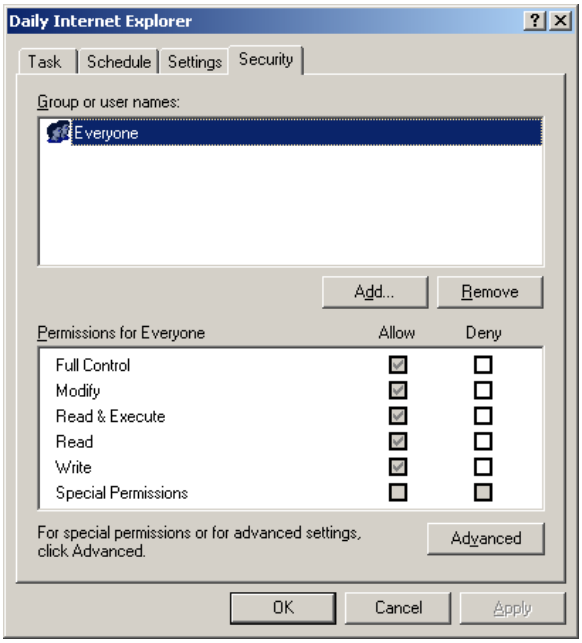


8. Click the **Settings** tab. On the Settings page, configure the task. For example, set it to **Stop the task if it runs for:** 0 hour(s) and 5 minute(s).



9. Click the **Security** tab to configure user and group permissions in order to allow or deny access to the scheduled task object that has just been created.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

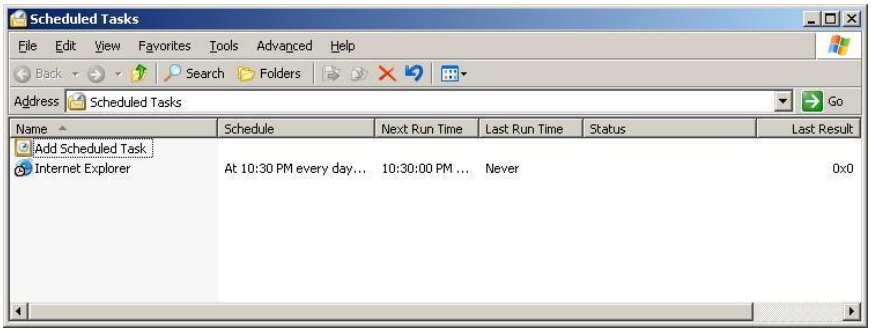


10. When finished, click **OK** to exit the Scheduled Task Wizard.

Modifying a Scheduled Task

Use the property pages of a scheduled task to modify a scheduled task.

1. Click **Start**, point to **Control Panel**, right-click on **Scheduled Tasks**, and then select **Open**.



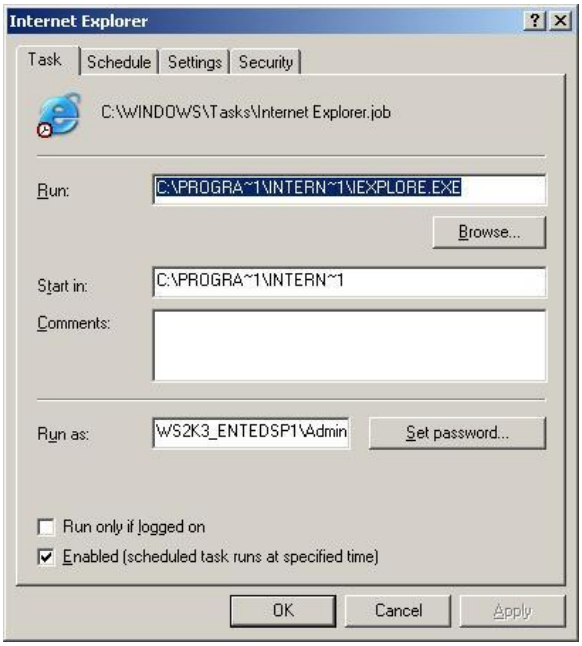
2. Right-click the task to be modified, and then click **Properties**. The Properties Interface appears and displays the **Task** tab by default. The **Task** tab gives the option to do one or more of the following:

   - To change a program being run, in **Run**, type the path for the new program.
   - To modify the startup folder for the program, type the new path in the **Start in** text box.
   - To change the user name that the task runs under, type the new user name in the **Run as** box and click **Set password**. Type the password twice, and click **OK** to return to the **Task** page.

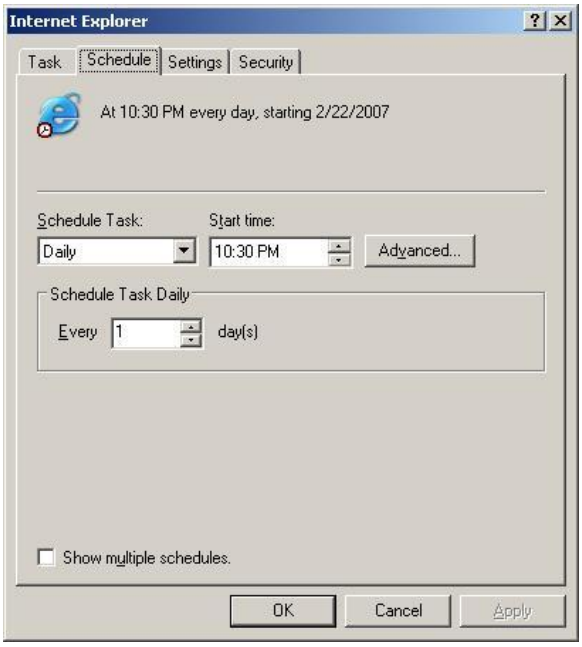
   Note: In the evaluated configuration, administrators can only schedule tasks for their own accounts.

   - If applicable, select the appropriate check boxes for **Run only if logged on** and **Enabled** (scheduled task runs at specified time)

Copyright © 2008 Microsoft Corporation.
All rights reserved.

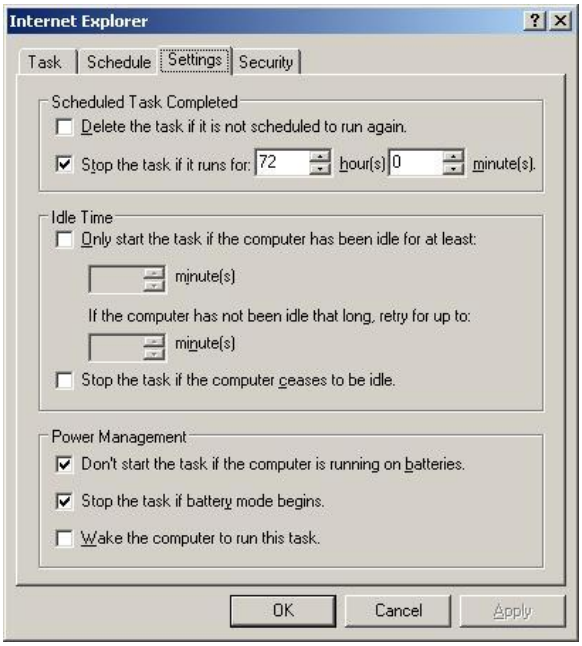


3. To change the schedule for the task, click the **Schedule** tab. The **Schedule** page gives the option to do one or more of the following:
   - Change the frequency of the task by clicking the drop-down list under **Schedule Task**. Choose from daily, weekly, monthly, once, at system startup, at logon, or when the system is idle.
   - Change the **Start time** of the task.
   - Change the recurrence of a daily task.
   - Configure and **Show multiple schedules** for the same task.



4. To customize the settings for the task, such as maximum run time, idle time requirements, and power management options, click the **Settings** tab.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

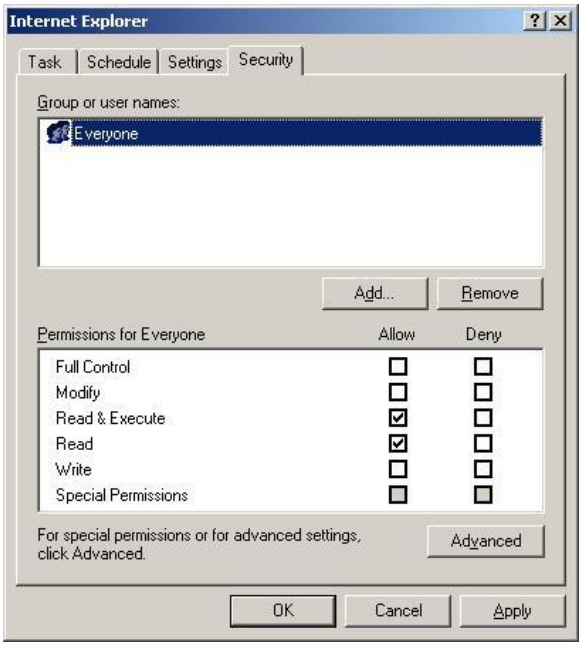


The **Settings** page gives the option to do one or more of the following.

- To delete a one-time task after it has run the final time, select the check box next to **Delete the task if it is not scheduled to run again**.
- To stop the task after it has run for a certain amount of time, type the number of **hours** and **minutes** in the appropriate boxes, and select the **Stop the task if it runs for <x> hours <x> minutes** check box.
- To start or stop a task based on when the computer becomes idle or ceases to be idle, select the appropriate check box in the **Idle Time** area.
- If the computer runs on batteries (such as a laptop), **Power Management** settings can be configured by selecting the appropriate check boxes near the bottom of the dialog box.

5. To configure access control permissions for the scheduled task, click the **Security** tab.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



6. Click **OK** to exit the properties pages of the scheduled task.

Removing a Scheduled Task

To remove a scheduled task:

1. Click **Start**, point to **Control Panel**, right-click on **Scheduled Tasks**, and then select **Open**.
2. Right-click the task to remove, and then select **Delete**.

Stopping or Starting a Scheduled Task

To stop a scheduled task that is running:

1. Click **Start**, point to **Control Panel**, right-click on **Scheduled Tasks**, and then select **Open**.
2. Right-click the task to remove, and then select **End Task**.
3. To start a scheduled task immediately, right-click the task to run, and then select **Run**.

Disabling Scheduled Tasks

To prevent scheduled tasks from running:

1. Click **Start**, point to **Control Panel**, right-click on **Scheduled Tasks**, and then select **Open**.
2. On the **Advanced** menu, select **Stop Using Task Scheduler**.

Viewing a Log of Past Scheduled Tasks

To view a log of past scheduled tasks:

1. Click **Start**, point to **Control Panel**, right-click on **Scheduled Tasks**, and then select **Open**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. On the **Advanced** menu, select **View Log**. The log file opens in Notepad.

The default log file for Scheduled Tasks is stored in the \Windows folder and is named SchedLgU.txt. When the log file reaches its maximum size, it automatically starts recording new information at the beginning of the log file and writes over old log file information.

Receiving Notification of Missed Tasks

To receive pop-up notification that some tasks might not have run at their specified time because Task Scheduler Service was stopped:

1. Click **Start**, point to **Control Panel**, right-click on **Scheduled Tasks**, and then select **Open**.
2. On the **Advanced** menu, select **Notify Me of Missed Tasks**.

Using the Scheduled Tasks command-line tool

The Scheduled Tasks command-line tool (Schtasks.exe) can be used to perform operations similar to those performed using Scheduled Tasks in Control Panel. Schtasks.exe can be used to create, delete, configure, or display scheduled tasks.

When a scheduled task is created using **Schtasks.exe /create**, an auditable object that has specific permissions assigned to it, a file with a .job extension, is created. An administrator can set permissions on that object.

No setup is required to run Schtasks.exe. Only administrator or member of the administrators group can run Schtasks.exe on the computer that the command affects. The Task Scheduler Service must be running and configured to **Log On as the Local System Account**.

There are six different parameters available to use with the Schtasks.exe command. To obtain usage information on each of the parameters listed below, open a command line interface and type `Schtasks /<ParameterName> /?`

- /Create Creates a new scheduled task.
- /Change Changes the properties of scheduled task.
- /Run Runs the scheduled task immediately.
- /End Stops the currently running scheduled task.
- /Delete Deletes the scheduled task(s).
- /Query Displays all scheduled tasks.

Using the AT scheduler tool

AT scheduler tool (AT.exe) is an automated task scheduler. It schedules commands and programs to run on a computer at a specified time and date. The Schedule service must be running to use the AT command. Membership in the Administrators group is required to schedule tasks using the AT command.

Although a newer version of the scheduling tool, Schtasks.exe, was developed to replace the AT command, the earlier tool is still available for use in Windows Server 2003. By default, AT.exe is stored in the %SystemRoot%\System32 folder.

To obtain usage information for the AT scheduler tool, open a command line interface and type `AT ?`

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Administering IPSec

IPSec policies, rather than Applications Programming Interfaces (APIs) or operations systems, are used to configure IPSec security services. The policies provide variable levels of protection for most traffic types in most existing networks. IPSec policies can be configured to meet the security requirements of a user, group, application, domain, site, or global enterprise. Microsoft Windows Server 2003 provides an administrative interface called **IPSec Policy Management** snap-in to define IPSec policies for computers at the Active Directory level for any domain members or on the local computer for non–domain members.

IPSec policies can be applied to computers, sites, domains, or any organizational units created in Active Directory. IPSec policies should be based on an organization's written (and unwritten) guidelines for secure operations. Through the use of security actions, called ***rules***, one policy can be applied to heterogeneous security groups of computers or to organizational units.

Notes: The Evaluated Configuration of the Windows Server 2003 family does not include the use of IPv6 with IPSec for the following reasons:

The implementation of IPSec for IPv6 relies on static keying and has no provisions for updating keys upon sequence number reuse.

IPSec in IPv6 is separate from and not interoperable with IPSec for the TCP/IP protocol. IPSec policies that are configured with the IP Security Policies or Group Policy snap-ins have no effect on IPv6 traffic.

IPSec in the IPv6 protocol for the Windows Server 2003 family does not support the use of data encryption for data confidentiality.

IPSec in the IPv6 protocol for the Windows Server 2003 family does not support the use of Internet Key Exchange (IKE) to negotiate Security Associations (SAs). IPSec policies, SAs, and keys must be manually configured.

There are two storage locations for IPSec policies:

- Active Directory. To securely manage an IPSec policy that is stored in Active Directory it must be managed from a Domain Controller.
- The local registry for stand-alone computers and computers which are not joined to the domain (when the computer is temporarily not joined to a trusted Microsoft Windows Server 2003 domain, the policy information is cached in the local registry).

Each policy should apply to a scenario considered in an organization's established security plan. Special configuration settings might apply if policies are assigned to a DHCP server, DNS, Windows Internet Name Service (WINS), Simple Network Management Protocol (SNMP), or remote access server.

Default IPSec Policy Templates

Computers that are connected to the Internet must be carefully protected from network attacks with custom policies. The default policies are defined as examples for intranets because they allow a computer to receive unsecured traffic. The default policies are designed for computers that are members of an Active Directory domain.

Warning: Windows Server 2003 provides a set of predefined IPSec filter lists, filter actions and default policies. These default IPSec policies are only intended as examples or as templates for creating new policies. They are not designed for operational use without prior modification. A knowledgeable IPSec network administrator should design new, custom polices for operational use.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Predefined Filter Lists

The following predefined filter lists are provided as examples for use in the default policies:

- **All ICMP Traffic**: A filter list for all Internet Control Message Protocol (ICMP) traffic (IP protocol 1) sent and received between this computer and all other computers.
- **All IP Traffic:** A filter list for all IP traffic sent and received between this computer and all other computers. All broadcast, multicast, and IKE traffic is excluded. By default, all Kerberos and Resource Reservation Protocol (RSVP) traffic is also excluded. However, authorized administrators can include Kerberos and RSVP traffic by editing the following registry key and adding the **NoDefaultExempt** value name with a value of 1:

Key Path: **HKLM\SYSTEM\CurrentControlSet\Services**		**Format**	**Value**
Key: IPSec	**Value Name:** NoDefaultExempt	REG_DWORD	1

Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Predefined Filter Actions

The following predefined filter actions are provided as examples for use in the default policies:

- **Permit**: Traffic is permitted (the security method is set to **Permit**).
- **Request Security (Optional)**: Traffic is secured (the security method is set to **Negotiate security**), however, the following exceptions apply:
  - Initial incoming unsecured communication is allowed. This behavior is known as inbound passthrough.
  - If security negotiation fails after 3 seconds, unsecured communication to a non-IPSec-aware computer is allowed. This filter action secures traffic to IPSec-aware computers, but allows unsecured communication if it is required. This behavior is known as fallback to clear.

  In order to avoid the potential for denial-of-service attacks, this filter action must not be used on the Internet.

  The following table lists the security methods (in preference order) for the **Request Security (Optional)** predefined filter action.

Type	Authentication Header (AH) integrity	Encapsulating Security Protocol (ESP) confidentiality	ESP integrity	Key lifetimes KiloBytes per Second (KB/sec)
Custom	None	3DES	SHA1	100000/900
Custom	None	DES	SHA1	100000/900
Custom	SHA1	None	None	100000/300
Custom	MD5	None	None	100000/300

The security negotiation for traffic using this filter action attempts ESP encryption (first 3DES, and then DES) with SHA1 integrity and then AH integrity (first SHA1, and then MD5).

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Require Security:** Traffic is secured (the security method is set to **Negotiate security**); however, initial incoming unsecured communication is allowed (inbound passthrough is enabled). Unsecured communication with non-IPSec-aware computers is not allowed (fallback to clear is disabled). For example, an incoming connection request packet is allowed. The computer's reply to the connection request matches the outbound filter, causing a request for security to be sent to the sender of the unsecured traffic. If security negotiation is successful, traffic in both directions is required to be secure. If security negotiation is not successful, outgoing traffic is not allowed. The computer might continue to receive incoming unsecured traffic and will continue to attempt to negotiate security.

  In order to avoid the potential for denial-of-service attacks, this filter action must not be used on the Internet.

  The following table lists the security methods (in preference order) for the **Require Security** predefined filter action.

Type	AH integrity	ESP confidentiality	ESP integrity	Key lifetimes (KB/sec)
Custom	None	3DES	SHA1	100000/900
Custom	None	3DES	MD5	100000/900
Custom	None	DES	SHA1	100000/900
Custom	None	DES	MD5	100000/900

  The security negotiation for traffic using this filter action will only attempt to negotiate ESP encryption (first 3DES, and then DES) with differing ESP authentication methods (first SHA1, and then MD5).

The most secure filter action is one that negotiates security and neither receives unsecured traffic (inbound passthrough is disabled) nor allows communication with non-IPSec-aware computers (fallback to clear is disabled). This is known as a lockdown filter action. When a server is using this filter action, clients must initiate secured communication before sending any IP traffic. The IPSec policy for client computers must be configured with additional rules that force the client to negotiate security with the server. A client configured with policy that consists of only the default response rule is not able to communicate with a lockdown server.

Predefined Rules

The only predefined rule that is available on all policies is the default response rule. The default response rule is automatically created in a new policy and cannot be created manually. It is used to respond to security requests when no other rule applies. For example, a client policy that enables a client to respond to security requests but does not secure any traffic by default would have only the default response rule active. In some cases, it is enabled by default. Administrators can disable the default response rule on the **Rules** tab in properties for a policy. Additionally, the authentication method and security methods of the default response rule can be modified for specific needs.

IPSec Policy Templates

The following are provided as examples for use in the default IPSec policies:

- **Client (Respond Only)**: This is an example policy for computers that secure communication on request. For example, intranet clients might not require IPSec except when requested by another computer. This policy enables the computer on which it is active to respond to requests for secured communications. This policy contains the default response rule, which creates dynamic IPSec filters for inbound and outbound traffic based on the requested protocol and port traffic for the communication that is being secured. This policy has the following settings:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Rule	Settings
First rule (default response rule)	IP Filter List: <Dynamic> Filter Action: Default Response Authentication: Kerberos Tunnel Setting: None Connection Type: All

- **Server (Request Security)**: This is an example policy for computers that should secure communications in most cases, allowing unsecured communication with non-IPSec-aware computers. With this policy, the computer accepts unsecured traffic, but always attempts to secure additional communications by requesting security from the original sender. This policy allows the entire communication to be unsecured if the other computer is not IPSec-enabled. For example, communication to specific servers can be secure while allowing the server to communicate in an unsecured manner to accommodate a mixture of clients (some of which support IPSec and some of which do not).

  To test the use of this policy, assign this policy to a server computer and assign the **Client (Respond Only)** policy to a client computer. When the client computer attempts to communicate with the server, the server requests secure communications. In addition, attempt to communicate with the server using a computer that either is not IPSec-capable or that has any IPSec policy assigned. When the non-IPSec-capable client attempts to communicate with the server, the server requests secure communications. However, the negotiation fails and the non-IPSec-capable computer connects to the server using unsecured communications.

  This policy has a rule to request security for all IP traffic, a rule to permit ICMP traffic, and the default response rule to respond to requests for security from other computers. This policy has the following settings:

Rule	Settings
First rule	IP Filter List: All IP Traffic Filter Action: Request Security (Optional) Authentication: Kerberos Tunnel Setting: None Connection Type: All
Second rule	IP Filter List: All ICMP Traffic Filter Action: Permit Authentication: Kerberos Tunnel Setting: None Connection Type: All
Third rule (default response rule)	IP Filter List: <Dynamic> Filter Action: Default Response Authentication: Kerberos Tunnel Setting: None Connection Type: All

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- **Secure Server (Require Security)**: This is an example policy for computers on an intranet that require secure communications, such as a server that transmits highly sensitive data. Administrators can use this IPSec policy as an example to create their own custom IPSec policy for production use. The filters used in this policy require all outbound communication to be secured, allowing only the initial inbound communication request to be unsecured.

  To test the use of this policy, assign this policy to a server computer and assign the **Client (Respond Only)** policy to a client computer. When the client computer attempts to communicate with the server, the server requests secure communications. In addition, attempt to communicate with the server using a computer that either is not IPSec-capable or that has any IPSec policy assigned. When the non-IPSec-capable client attempts to communicate with the server, the server requests secure communications. However, the negotiation fails and the non-IPSec-capable computer does not connect to the server.

  This policy has a rule to require security for all IP traffic, a rule to permit ICMP traffic, and the default response rule to respond to requests for security from other computers.

Rule	Settings
First rule	IP Filter List: All IP Traffic Filter Action: Require Security Authentication: Kerberos Tunnel Setting: None Connection Type: All
Second rule	IP Filter List: All ICMP Traffic Filter Action: Permit Authentication: Kerberos Tunnel Setting: None Connection Type: All
Third rule (default response rule)	IP Filter List: <Dynamic> Filter Action: Default Response Authentication: Kerberos Tunnel Setting: None Connection Type: All

IPSec Policy Components

Security administrators may want to create their own policy to suit their particular security needs and requirements. One way to do this is by using the **IP Security Policy Wizard**. The IP Security Policy Wizard can be used to set the following:

Filters: IPSec uses IP packet filtering methodology as the basis for determining whether communication is allowed, secured, or blocked, according to the IP address ranges, protocols, or even specific protocol ports.

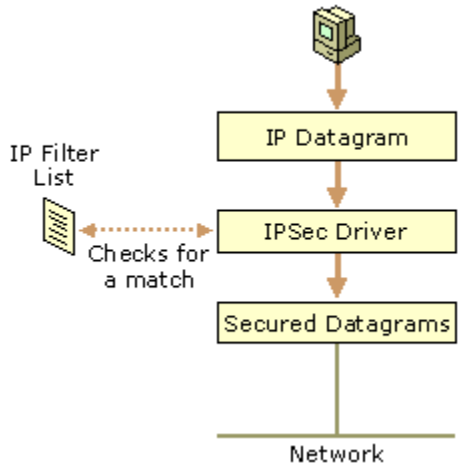
IPSec provides access control by enabling an administrator to designate specific filters and filter actions in an IPSec policy. Two types of access control are provided: simple IP packet filtering and successful authentication. Additionally, permit and block actions allow control over the type of IP packets a computer may send or receive or the addresses with which a computer may communicate.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

IPSec Driver: The IPSec driver, using the IP Filter List from the active IPSec policy, watches for outbound IP packets that must be secured and inbound IP packets that need to be verified and decrypted.

As shown in the following diagram, the IPSec driver receives the IP filter list from the IPSec policy agent. The IPSec driver watches all outgoing IP packets on the computer for a match with the stored IP filter list. Outbound packets initiate the negotiation for security when a match occurs. The IPSec driver notifies IKE to begin security negotiations.



Rules: Rules govern how and when an IPSec policy protects communication. A rule provides the ability to trigger and control secure communication based on the source, destination, and type of IP traffic. It associates a filter with a filter action and is defined by the IPSec policy.

Each rule contains a list of IP filters and a collection of security actions that take place upon a match with that filter list:

- Filter actions
- Authentication methods
- IP tunnel settings
- Connection types

Each policy can contain one rule, or multiple rules, all of which can be active simultaneously. For example, security administrators might want to have one policy for a site router, but require different security actions for intranet and Internet communications. One policy can be used for the router by creating multiple rules, one for each possible communication scenario.

Default rules are provided with IPSec, encompassing a variety of client and server-based communications. These can be used as is, or modified to meet specific requirements.

IP Packet Filtering: An IP address identifies a computer system's location on the network. Each IP address is separated internally into two parts, a network ID and a computer ID:

- The network ID identifies a single network within a larger TCP/IP network (that is, a network of networks). This ID is also used to identify each network uniquely within the larger network.
- The computer ID for each device (such as a workstation or router) identifies a system within its own network.

Multi-homed computers have multiple IP addresses, one for each network adapter.

Filters: A rule provides the ability to trigger security negotiations for communication based on the source, destination, or type of IP traffic using a process called IP packet filtering. This provides a way to define precisely the IP traffic that will be secured, blocked, or passed through (unsecured).

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Each filter within an IP Filter List describes a particular subset of network traffic to be secured, both for inbound and outbound traffic:

- **Inbound filters** apply to traffic received, allowing the receiving computer to match the traffic with the IP filter list. Inbound filters respond to requests for secure communication or match the traffic with an existing Security Association (SA) and process the secured packets.
- **Outbound filters** apply to traffic leaving a computer toward a destination and trigger a security negotiation that must take place before traffic is sent.

A filter must be available to cover any traffic for which the associated rule is applied. For example, if Computer "A" always wants to exchange data securely with Computer "B:"

- In order to send secured data to Computer B, Computer A's IPSec policy must have a filter for any outbound packets going to Computer B.
- In order to receive secured data from Computer A, Computer B's IPSec policy must have a filter for any inbound packets from Computer A.

A filter contains the following parameters:

- The source and destination address of the IP packet. These can be configured from a very detailed level, such as a single IP address, to a global level that encompasses an entire subnet or network.
- The protocol over which the packet is being transferred. This defaults to cover all protocols in the TCP/IP protocol suite. The filter can be configured to an individual protocol level to meet special requirements including custom protocol numbers, however, this is not included in the evaluated configuration.

Note: IPSec policies configured to apply to the Transport Mode of communication only are included in the Evaluated Configuration.

- The source and destination port of the protocol for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). This also defaults to cover all ports but can be configured to apply to only packets sent or received on a specific protocol port.

Filter Actions: The filter action sets the security requirements for the communication. These requirements are specified in a list of security methods contained in the filter action, including which algorithms, security protocols, and key properties are to be used.

A filter action can also be configured with the following policies:

- **Pass-through policy (Permit)**. This does not provide for secure communication. IPSec simply ignores traffic in this case. This is appropriate for traffic that cannot be secured because the remote computer is not IPSec-enabled, traffic that is not sensitive enough to require protection, or traffic that provides its own security.
- **Blocking policy (Block)**. This stops communication from a certain address or group of addresses.
- **Negotiating Policy (Negotiate Security)**. A policy that negotiates for security but still enables communication with non-IPSec-enabled computers. A filter action can be configured to use fall back to clear. If there is a need to configure a filter action like this, limit the IP filter list to a minimal scope. However, it should be used with extreme caution. Any communications affected by that policy could result in data being sent without protection if negotiation fails for any reason. If the initiator of an IKE negotiation receives a reply from the responder, then the negotiation does not allow fallback to clear.

Some recommendations for filter actions:

- If there is a need to prevent communication with rogue computers, ensure that security is not negotiated for nonessential data or when peers are not IPSec-enabled—make use of filter actions such as blocking or pass-through policies.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- When configuring custom security methods, only set the ESP confidentiality selection to None when a higher layer protocol will provide data encryption.
- For remote communication scenarios (including IPSec tunneling), consider a list of security methods that specifies high levels of security, such as 3DES only, short key lifetimes (less than 50 MegaBytes (MBs)), and perfect forward secrecy for the master and session keys. This helps protect against known-key attacks.

IP Filter Lists: Here are some recommendations for IP filter lists:

- Try to use general filters if there is a need to cover a group of computers with only one filter. For example, in the Filter Properties interface, use Any IP Address or an IP subnet address rather than specifying a specific computer's source and destination IP address.
- Define filters that allow grouping and securing traffic from logically associated segments of the network.
- The order in which the filters apply is not related to the ordering displayed when viewing the IPSec policy. All filters are simultaneously retrieved by the IPSec Policy Agent during system startup, and are processed and sorted from most specific to least specific. There is no guarantee that a specific filter will be applied before a general filter until all the filters have been processed, and that may affect some communications behavior during system startup.

Configuring IPSec Policies

There are two storage locations for IPSec policies:

- Active Directory. If the computer is temporarily unconnected to a trusted Windows Server 2003 domain, the policy information is cached in the local registry.
- The registry on a local computer. Local IPSec policies are defined in the registry for stand-alone computers and computers that are not always part of a trusted Windows Server 2003 domain.

A network security administrator can configure IPSec policies to meet the security requirements of a domain, site, or organizational unit for an Active Directory domain. IPSec policy can also be implemented in a non-Active Directory domain environment by using local IPSec policies.

Group Policy

IPSec policies, which are assigned to a Group Policy object in Active Directory, become part of Group Policy, and are transferred to the member computers each time Group Policy propagates.

When assigning an IPSec policy in Active Directory, consider the following:

- IPSec policies that are assigned at the domain level override any active, local IPSec policy when that computer is joined to the domain.
- IPSec policies that are assigned to an organizational unit override an IPSec policy assigned at the domain level, for any member computers of that organizational unit. The IPSec policy assigned to the lowest-level organizational unit in the domain hierarchy overrides an IPSec policy assigned to a higher-level organizational unit, for any member computers of that organizational unit.

Create an IPSec Policy for a Windows Server 2003 Domain

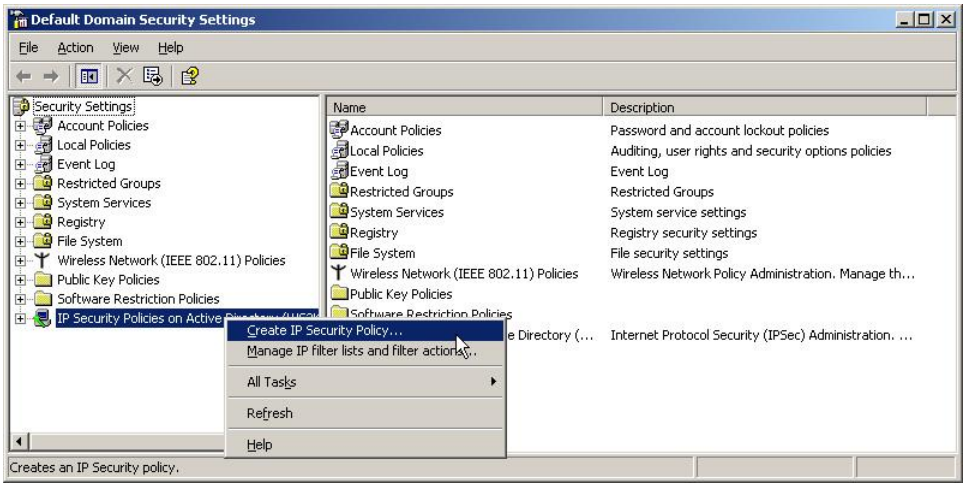
1. Log on to the Domain Controller as an authorized administrator.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: The procedures below demonstrate the use of the Domain Security Policy to create an existing IPSec policy to a domain. The procedures are similar when creating an IPSec policy through a Local Security Policy interface for stand-alone or member servers, or when creating an IPSec policy using a site or OU GPO.

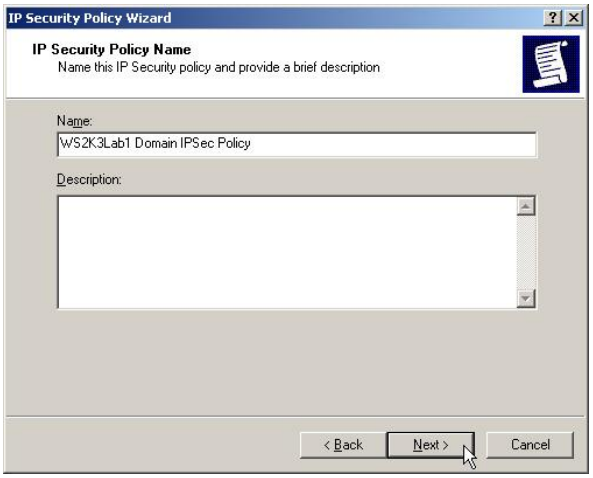
2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Security Settings**, right-click **IP Security Policies on Local Computer**, and then select **Create IP Security Policy**. The **IP Security Policy Wizard** appears.



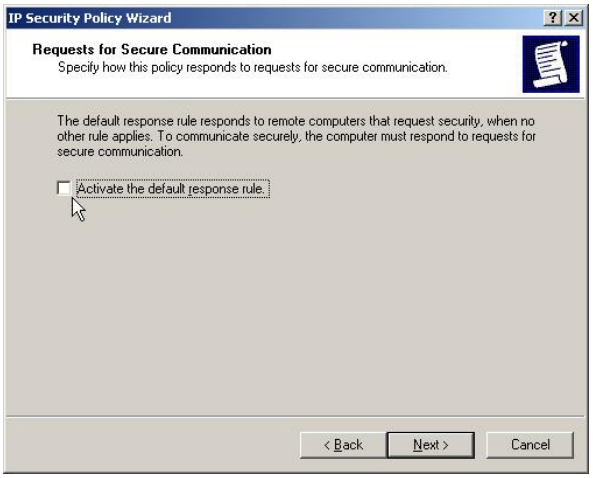
4. Click **Next**.

5. Type the name of the policy, and click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



6. Clear the Activate **the default response rule** check box, and then click **Next**.

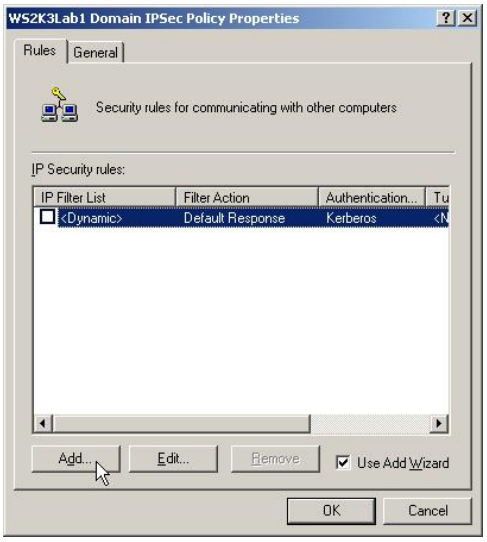


7. Make sure the **Edit Properties** check box is selected (it is by default), and then click **Finish**.

8. In the **Properties** interface for the policy just created, ensure that the **Use Add Wizard** check box in the lower-right corner is selected, and then click **Add** to start the **Security Rule Wizard**.

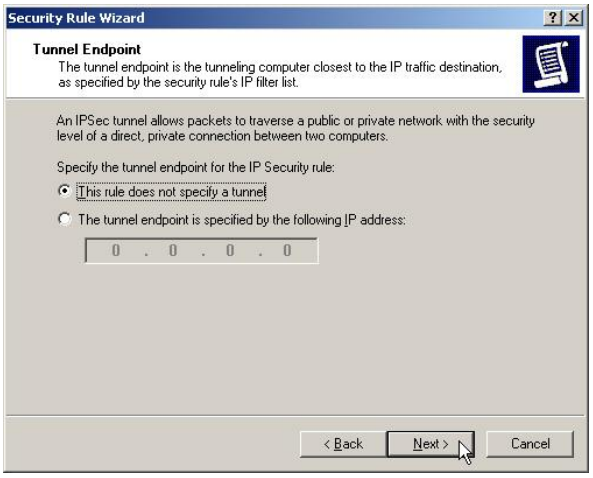
Copyright © 2008 Microsoft Corporation.

All rights reserved.



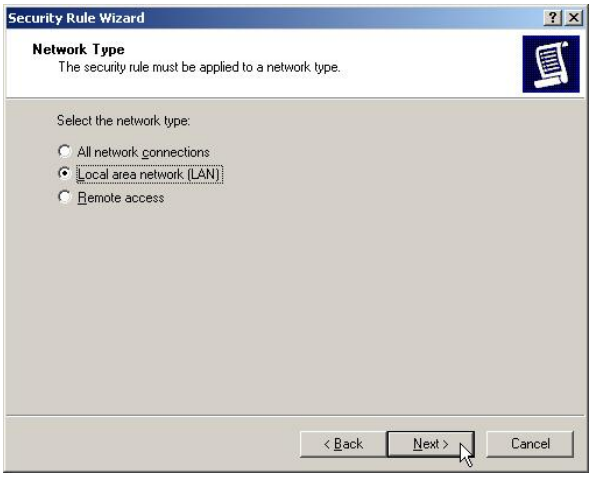
9. Click **Next** to proceed through the **Security Rule Wizard**.

10. In the **Tunnel Endpoint** selection window of the **Security Rule Wizard**, decide whether tunneling will be enabled. Select **This rule does not specify a tunnel** (selected by default) to disable tunneling for this rule, or select **This tunnel endpoint is specified by the IP address** and then enter the IP address of the computer that is the specific tunnel end point. For this example, select **This rule does not specify a tunnel** and click **Next**.

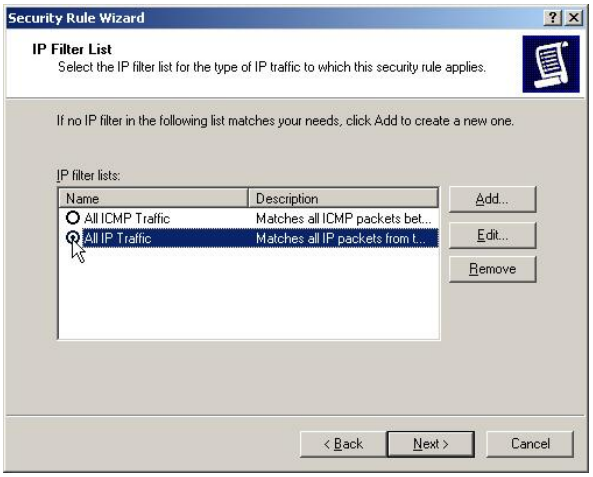


Copyright © 2008 Microsoft Corporation.
All rights reserved.

11. In the **Network Type** selection window of the **Security Rule Wizard**, decide the type of network environment that the rule will be applied to. Select **All network connections** apply the rule to all networks whether local or external, select the **Local area network (LAN)** to apply the rule to all connections from the local network, or select **Remote access** to apply the rule to dial-up connections. For this example, select **Local area network (LAN)** and click **Next**.



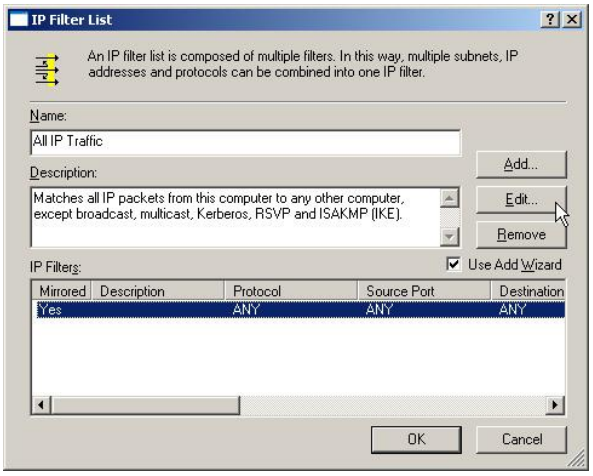
12. Select an IP filter for the type of traffic to which the rule is to apply. Select from one of the two default filters and click **Edit** to modify the filter as needed. Otherwise, click **Add** to create a new filter. For this example, select the **All IP Traffic filter** and click the **Edit** button.

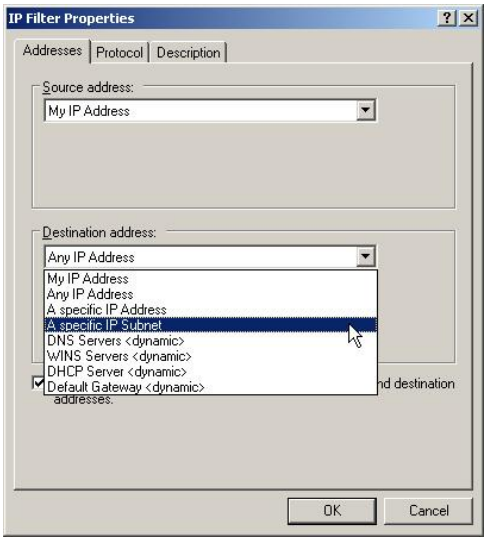


13. The **IP Filter List** interface will appear. To edit the default filter, select the filter and click the **Edit** button to make necessary changes in the **IP Filter Properties** interface.

Copyright © 2008 Microsoft Corporation.

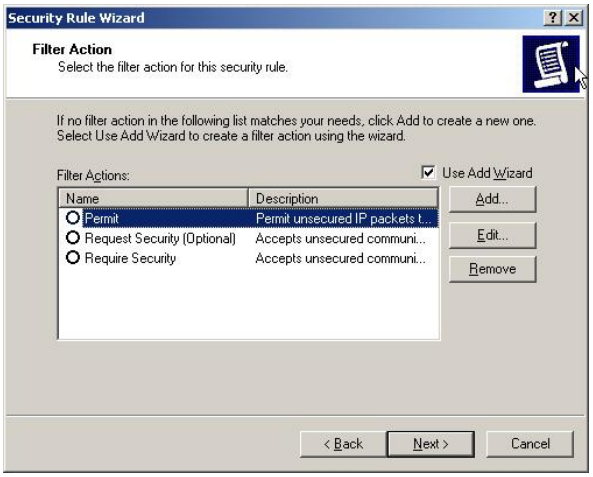
All rights reserved.





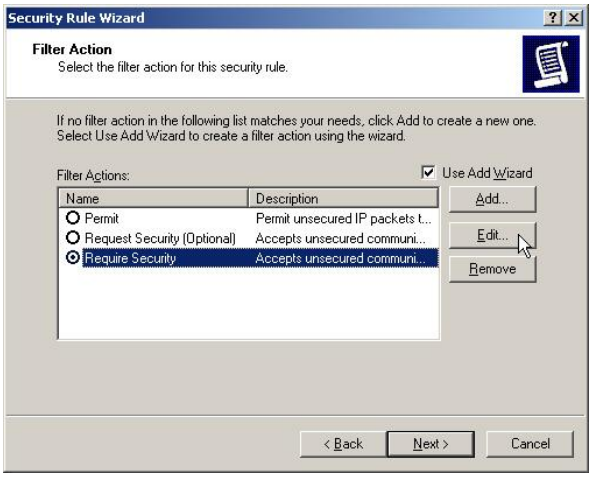
14. The **IP Filter List** may be composed of multiple filters. To add a filter, make sure the **Use Add Wizard** check box is selected in the IP Filter List interface and click the **Add** button. Follow the **IP Filter Wizard** instructions to create a new filter.

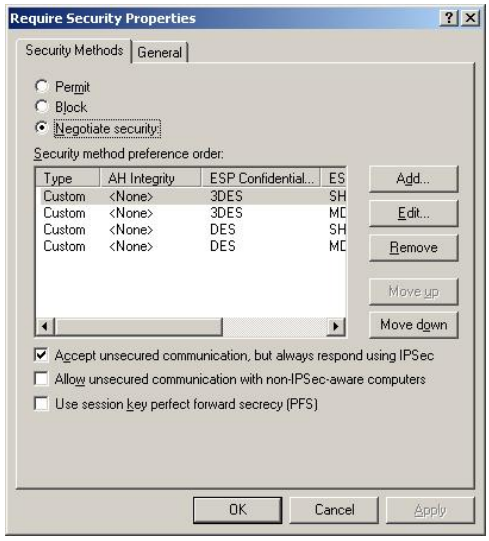
15. Once all edits are completed, click **OK** on the **IP Filter List** interface. Click **Next** on the **Security Rule Wizard**. In the **Filter Action** selection window will appear.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

16. Select a filter action for the security rule from one of the default actions presented. To edit a filter action, click the **Edit** button. To create a new filter action, make sure the **Use Add Wizard** check box is selected and click the **Add** button. For this example, select the **Require Security** action and click the **Edit** button. The Require Security Properties interface will appear. Make changes as necessary and click **OK** to return to the **Filter Action** selection window.





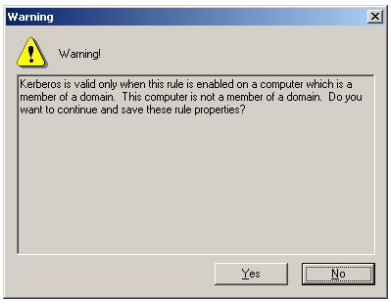
17. To add a new filter action for the security rule, make sure the **Use Add Wizard** check box is selected in the **Filter Action** selection window and click the **Add** button. Follow the **IP Filter Wizard** instructions to create a new filter.

18. Click **Next** on the **Security Rule Wizard**. In the **Authentication Method** selection window of the **Security Rule Wizard**, decide on one of the following authentication methods:

    - Select **Active Directory default (Kerberos V5 protocol)** to use the Kerberos V5 security protocol for authentication services, if this rule applies to computers that are validated by a Windows Server 2003 Active Directory domain or a trusted Active Directory domain. If this authentication method is selected on a computer that is not a domain member, a warning message will appear stating that this rule will only be enabled on computers that are members of an Active Directory domain.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

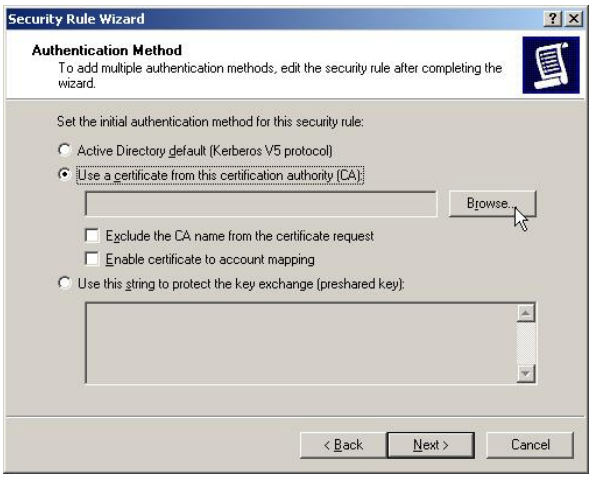


To use Kerberos, the computers must:

- Be part of the same domain and forest
- Be within a specific source address range
- Be within the same subnet
- Use static IP addresses
- To use a public key certificate for authentication services, select **Use a certificate from this Certification Authority (CA)**, and then click Browse to select a root CA. To use certificate authentication, the two computers must trust a common CA, and the server that performs the authentication must request and install a certificate from the CA.
- To specify a specific key that will be used for authentication, select **Use this string to protect the key exchange (preshared key)**. To use pre-shared secret-key-based authentication, the two computers must share an encryption key.

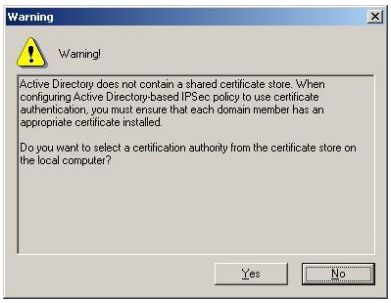
Note: For the Evaluated Configuration the use of pre-shared keys is not allowed. By default, an IPSec policy that is stored in Active Directory can be read by any authenticated user, but changed only by directory administrators. Because of this, specifying an authentication key value in directory-based policy is not allowed in the Evaluated Configuration. Since the pre-shared key value is stored in readable format within the IPSec policy, the local use of pre-shared keys is also not allowed in the Evaluated Configuration.

19. For this example, select **Use a certificate from this certification authority (CA)** and click the **Browse** button to select a **CA**.

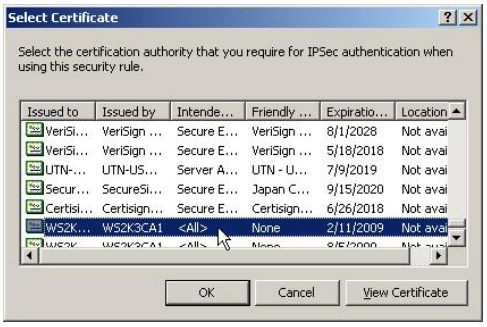


20. On a Domain Controller, a warning message may appear indicating that Active Directory does not contain a shared certificate store. Click **Yes**.

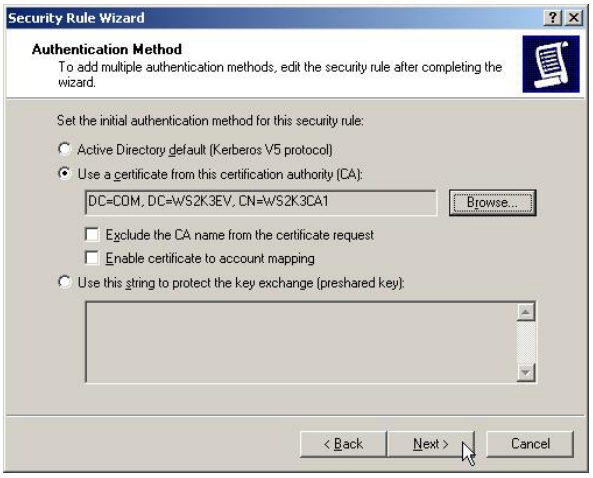
Copyright © 2008 Microsoft Corporation.
All rights reserved.



21. Select a CA certificate from the **Select Certificate** interface. To view the certificate, click the **View Certificate** button. Click **OK** on the **Select Certificate** interface.



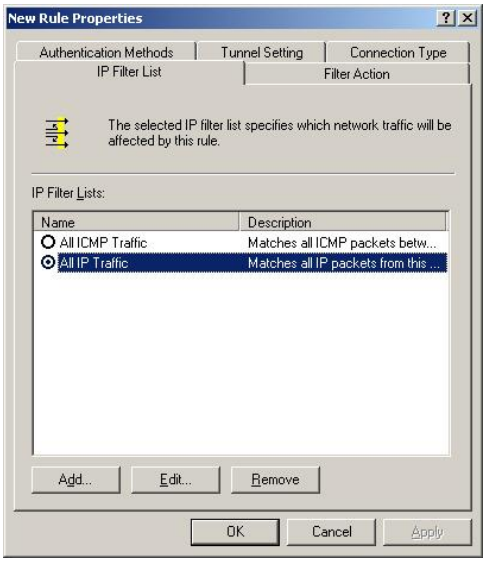
22. Click **Next** on the **Authentication Method** selection window of the **Security Rule Wizard**.



23. To edit the security rule, check the **Edit properties** box and click **Finish**.

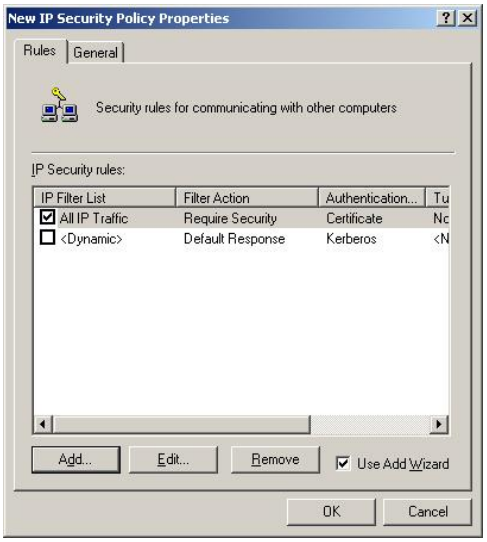
Copyright © 2008 Microsoft Corporation.
All rights reserved.

24. If the **Edit properties** check box was selected on the **Security Rule Wizard**, the **New Rule Properties** interface will appear to allow additional modifications. Once any needed modifications are made, click **OK** to close the **New Rule Properties** interface.

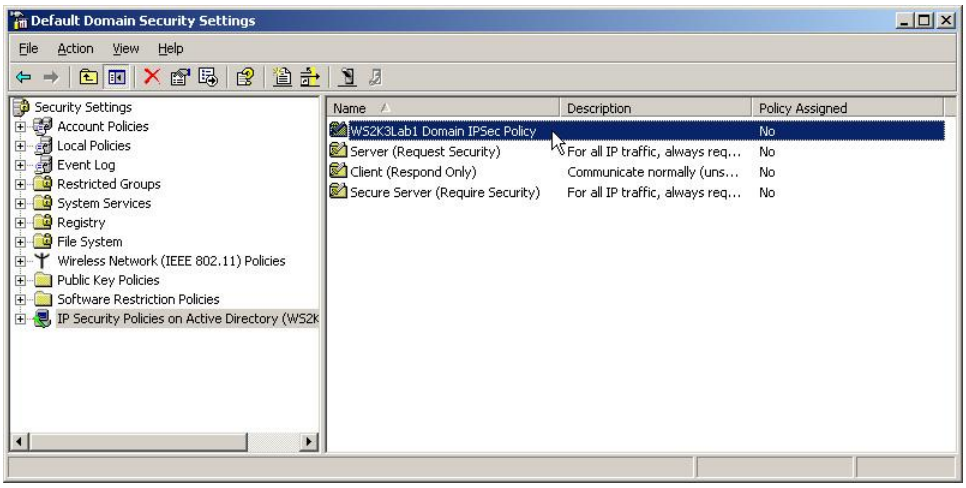


25. Click **Close** on the **Properties** window for the new IP Security Policy.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



26. The newly created IP Security Policy will appear as a new selection in the **Local Security Policy** interface, but is not yet assigned.



Assign an IP Security Policy to a Windows Server 2003 Domain

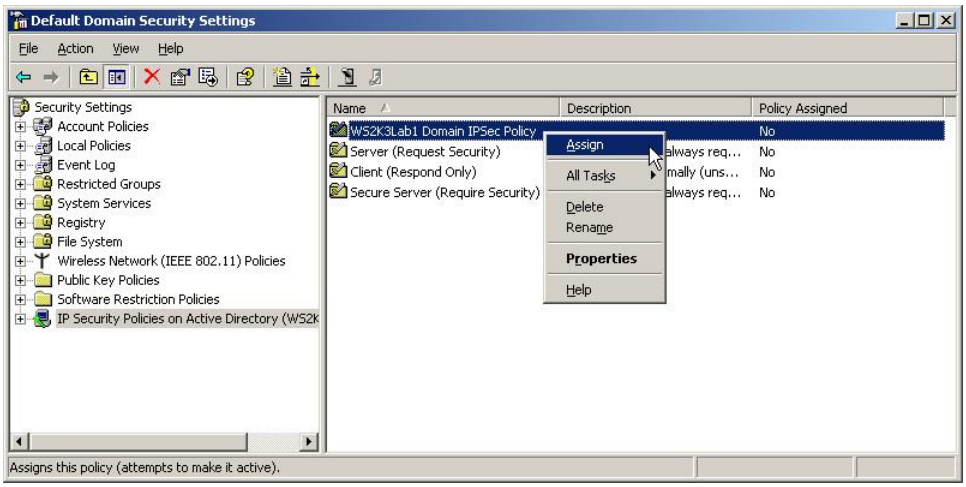
To assign an existing IPSec Policy to a Windows Server 2003 domain:

1. Log on to the Domain Controller as an authorized administrator.

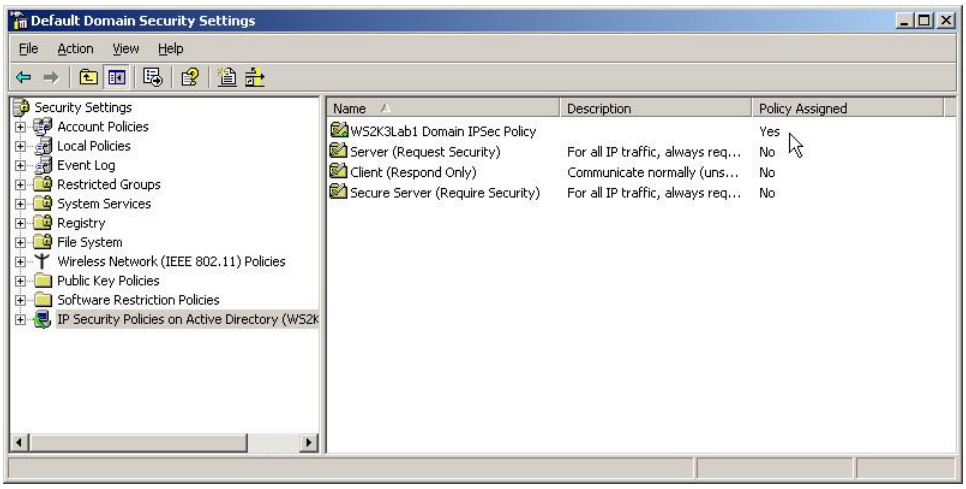
   Note: The procedures below demonstrate the use of the Domain Security Policy assign an existing IPSec policy to a domain. The procedures are similar when assigning an IPSec policy through a Local Security Policy interface for stand-alone or member servers, or when using a site or OU GPO.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Security Settings** and select **IP Security Policies on Local Computer** to display the available policies in the details pane.
4. Right-click on the policy to assign and choose **Assign** from the menu.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. This changes the **Policy Assigned** field in the details pane to **Yes**.



Edit and Existing IP Security Policy

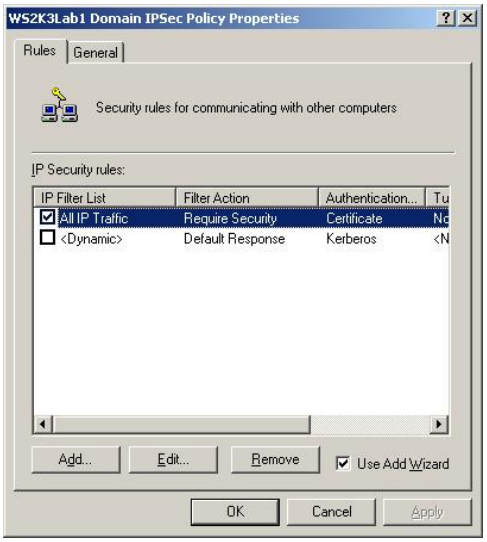
1. Log on to the Domain Controller as an authorized administrator.

   Note: The procedures below demonstrate the use of the Domain Security Policy to edit an existing IPSec policy for a domain. The procedures are similar when editing an IPSec policy through a Local Security Policy interface for stand-alone or member servers, or when using a site or OU GPO.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Expand **Security Settings** and select **IP Security Policies on Local Computer** to display the available policies in the details pane.
4. Double-click the policy that is to be modified. The **Properties** interface for the policy will appear. Make changes as necessary. The procedures will be similar to those presented above for creating a new IPSec Policy.

Copyright © 2008 Microsoft Corporation.

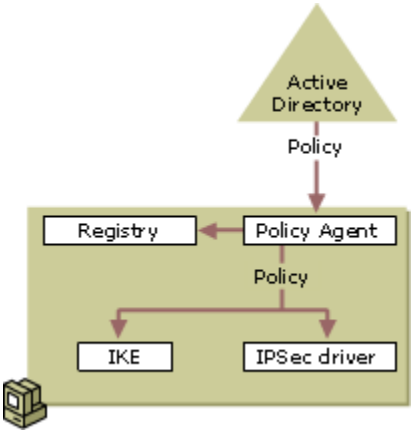
All rights reserved.



5. When all changes are completed, close the **Properties** interface by clicking the **OK** button.

IPSec Policy Agent Service

The purpose of the IPSec Policy Agent is to retrieve policy information and pass it to other IPSec components that require this information to perform security services, as shown in the following illustration.



The IPSec Policy Agent is a service that resides on each Windows Server 2003 computer, appearing as **IPSec Services** in the list of system services in the Services snap-in. The IPSec Policy Agent performs the following tasks:

- Retrieves the appropriate IPSec policy (if one has been assigned) from Active Directory, if the computer is a domain member, or from the local registry, if the computer is not a member of a domain.
- Polls Active Directory for changes in policy configuration (for domain-based policy).
- Sends the assigned IPSec policy information to the IPSec driver.

Retrieval of the policy occurs at system start time, at the interval specified in the IPSec policy (if the computer is joined to a domain), and at the default Winlogon polling interval (if a joined to a domain). The following are additional aspects of IPSec policy behavior for a computer that is a member of a domain:

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- If IPSec policy information is centrally configured for computers that are domain members, the IPSec policy information is stored in Active Directory and cached in the local registry of the computer to which it applies.
- If the computer is temporarily not connected to the domain and policy is cached, new policy information for that computer replaces old, cached information when the computer reconnects to the domain.
- If the computer is a stand-alone computer or a member of a domain that is not using Active Directory for policy storage, IPSec policy is stored in the local registry.

The IPSec Policy Agent starts automatically at system start time. If there are no IPSec policies in Active Directory or the registry, or if the IPSec Policy Agent cannot connect Active Directory, the IPSec Policy Agent waits for policy to be assigned or activated.

Firewalls and IPSec

If a firewall separates two hosts that use IPSec to secure the communication channel, the firewall must open the following ports:

- TCP port 50 for IPSec ESP traffic
- TCP port 51 for IPSec AH traffic
- UDP port 500 for IKE negotiation traffic

Implementing the Encrypting File System in Windows Server 2003

EFS is the file encryption technology used for NTFS volumes. It runs as a service and takes advantage of the Cryptographic API (CryptoAPI) architecture in Windows Server 2003. The default configuration of EFS requires no administrative effort; users are allowed to encrypt files by default. The first time EFS is used, it automatically generates an encryption key pair and a certificate for the user if one does not exist already.

EFS can use either the AES or 3DES as the encryption algorithm. The default algorithm for Windows XP SP1 and higher and Windows Server 2003 is AES using a 256-bit key. For users requiring greater symmetric key strength with Federal Information Processing Standards (FIPS) 140-1 compliant algorithm, the 3DES algorithm can be enabled.

EFS Enhancements in Windows XP and Windows Server 2003

Microsoft Windows 2000 introduced the capability for data protection and protected data recovery with the implementation of EFS, and this capability has been enhanced in Windows XP and Windows Server 2003. The new EFS enhancements include:

- Full support for revocation checking on certificates used when sharing encrypted files
- Support for EFS with Windows Server 2003 clusters
- Support for encrypted offline folders in Windows XP
- Multi-user support for encrypted files in the shell User Interface (UI)
- Support for Microsoft Enhanced and Strong Cryptographic Service Providers (CSPs)
- Additional support for enhanced algorithm options and strengths
- End-to-end encryption using EFS over WebDAV

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Enhanced recovery policy flexibility
- Performance and reliability enhancements
- Additional security features for protecting EFS data

Components of EFS

EFS consists primarily of the following operating system components: the EFS service and EFS Run-Time Library. The EFS Run-Time Library is an internal library of NTFS.SYS driver providing NTFS the EFS functionalities and an API. Like many other security services, EFS uses the Microsoft CryptoAPI to obtain services from a CSP such as the RSA Base Provider that is included with Windows Server 2003.

EFS Service. The EFS service is part of the security subsystem. It uses the existing Local Procedure Call (LPC) communication port between the Local Security Authority (LSA) and the kernel-mode security reference monitor to communicate with the EFS Run-Time Library. In user mode, it interfaces with CryptoAPI to obtain file encryption keys and to generate Data Decryption Fields (DDFs) and Data Recovery Fields (DRFs). The EFS service also provides support for Win32 APIs.

The EFS service calls CryptoAPI to acquire the file encryption key (FEK) for a data file and then to encode the FEK, thus producing the DDF. The EFS service also returns the FEK, DRF, and DDF by way of the EFS Run-Time Library.

CryptoAPI. EFS uses CryptoAPI for all of its cryptographic operations. CryptoAPI provides services that enable application developers to add cryptography to their Win32 applications. CryptoAPI consists of a set of functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for private key data. Applications can use the functions in CryptoAPI without knowing anything about the underlying implementation.

CryptoAPI provides the underlying security services for secure channels and code signing. CryptoAPI supports public key and symmetric-key operations such as key generation, key management and secure storage, key exchange, encryption, decryption, hashing, digital signatures, and verification of signatures. Developers can use certificates with these public key operations and perform the necessary encapsulations and encoding to apply certificates within their applications.

CSP. By default, EFS uses the AES algorithm with a 256-bit key in Windows Server 2003. The public-private key pairs for EFS users and recovery agent accounts are obtained from the Microsoft base CSP, also called the RSA base provider. This CSP is included with Windows Server 2003 and is approved for general export worldwide. The Microsoft enhanced CSP can also be used for EFS.

Windows Server 2003 can be configured to use the 3DES algorithm instead of AES. 3DES is compliant with FIPS 140-2 Level 1 and provides encryption using a 168-bit key.

> **Note:** The FIPS 140-2 is a security implementation designed for certifying cryptographic software. FIPS 140-2 validated software is required by the U.S. Government and requested by other prominent institutions.

Data Protection API. The Data Protection API (DPAPI) is a set of function calls that provide data protection services to user and system processes. Applications either pass plaintext data to DPAPI and receive protected data back, or pass the protected data to DPAPI and receive plaintext data back. For example, after a CSP generates keys for certificates, it calls CryptProtectData(), one of the primary functions of DPAPI, to protect those keys. When the keys are needed, DPAPI decrypts them.

Win32 API. EFS provides an API set to expose its features. This API provides a programming interface for operations such as encrypting plaintext files, decrypting or recovering ciphertext files, and importing and exporting encrypted files (without decrypting them first). The API is remoted to support remote encryption, decryption, backup, and restore operations. The API is supported in a standard system DLL, Advapi32.dll.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Enabling 3DES

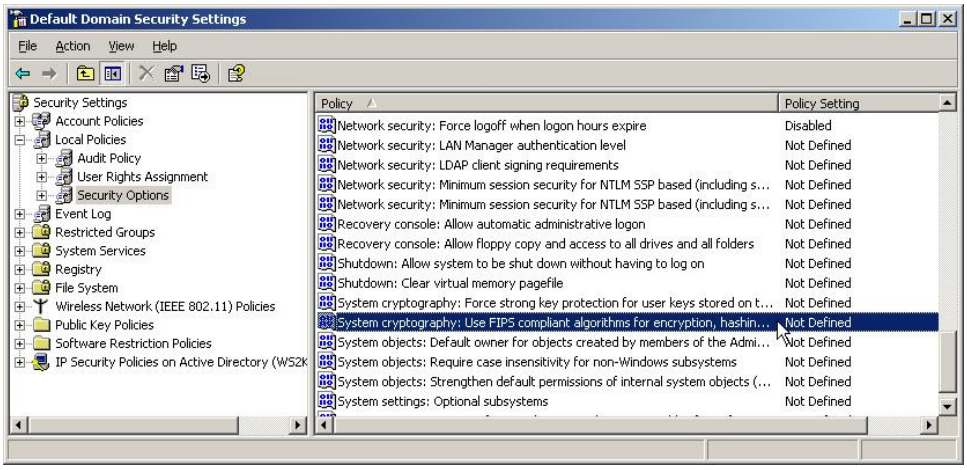
In the Evaluated Configuration, 3DES encryption is enabled. Authorized administrators can verify that 3DES is enabled, or can enable 3DES on systems that have not yet been fully configured, by using the **System cryptography: Use FIPS compliant algorithms for encryption** Security Option in the Local Security Policy, or on a domain-based security policy. When this setting is configured for 3DES, IPSec and EFS both use 3DES for encryption.

To enable system-wide 3DES for systems within a domain by using **Domain Security Policy**:

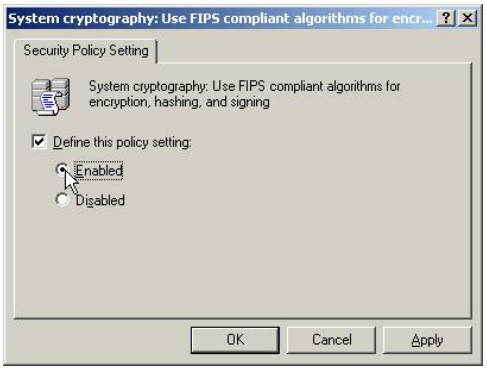
1. Log on to the Domain Controller as an authorized administrator.

   Note: The procedures below demonstrate use of the **Domain Security Policy** to push the **System cryptography: Use FIPS compliant algorithms for encryption** setting across a domain. The procedures are similar when using a Local Security Policy interface for stand-alone or member servers, or using a site or OU GPO.

2. Click **Start**, point to **Administrative Tools**, and then select **Domain Security Policy**. This opens the **Default Domain Security Settings** interface.
3. Under **Security Settings**, expand **Local Policies**.
4. Select **Security Options**, to see a list of security option policies in the right-hand details pane.
5. In the details pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption**.



6. Check the **Define this policy setting** check box, select **Enabled**, and then click **OK**.



7. If there are no other changes to be made to the Domain Security Policy, close the **Default Domain Security Settings** interface and restart the computer.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Changing the Default RSA Key Sizes for Keys Generated for EFS

Windows Server 2003 supports the ability specify larger default RSA key sizes for keys generated for EFS. The default key size used by Windows XP and Windows 2003 is 1024 bits with the Microsoft Base Provider. With Windows Server 2003, this default size can be changed by setting the following registry key with a DWORD value as specified below. If the number is larger than 16384, it will be ignored. If the number is not a multiple of eight (8), it will be reduced to the next multiple of eight (8). If the length is greater than 1024, the Microsoft Enhanced Provider CSP will be used for generating the key.

Key Path: **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion**	**Format**	**Value**
Key: EFS **Value Name:** RSAKeyLength	REG_DWORD	Set to a value between 1024 and 16384

Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

Maintaining File Confidentiality

Only authorized users and designated DRAs can decrypt encrypted files. Other system accounts that may have NTFS permissions for a file, including the **Take ownership of files or other objects** privilege, cannot open the file without authorization. Even the administrator account cannot open the file if that account is not designated as a data recovery agent. If an unauthorized user tries to open an encrypted file, access will be denied. Authorization to open an encrypted file can be granted to a user by the file owner by adding the user's certificate to the encrypted file.

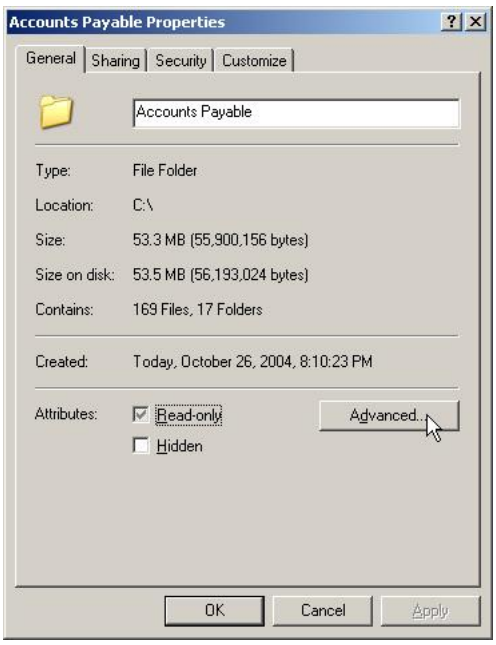
Encrypting a File or Folder

If a folder is encrypted, all files and subfolders created in, or added to, the encrypted folder are automatically encrypted. It is recommended that encryption be done at the folder level to prevent plain-text temporary files from being created on the hard disk during file conversion. Encrypt a file or folder on an NFTS volume as follows:

1. Select the file or folder to encrypt.
2. Right-click on the file or folder and click **Properties**.
3. On the **General** tab, click **Advanced**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



4. On the **Advanced Attributes** interface, select the **Encrypt contents to secure data** check box and click **OK**. Notice that the **Details** button is grayed out.

Note: A file cannot be both compressed and encrypted at the same time.

5. Click **OK** in the **Properties** interface.
6. A **Confirm Attributes Changes** dialog will ask to choose between encrypting the folder and all its contents or just the folder itself. If the folder is empty, choose to encrypt the folder only; otherwise, choose the folder and its contents, and click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

7. An interface shows the progress status of encrypting the folder or file. Click **OK** again to make this change, and close the **Properties** interface.

Note: When an encrypted file is moved to another folder that is not encrypted, the file remains encrypted. However, if the owner of the file moves the file to a FAT partition or volume, such as a floppy disk, the file is automatically decrypted.

8. The display name for all encrypted files and folders will be presented in green text. This allows users to easily identify encrypted files and folders.

Obtaining EFS Certificates

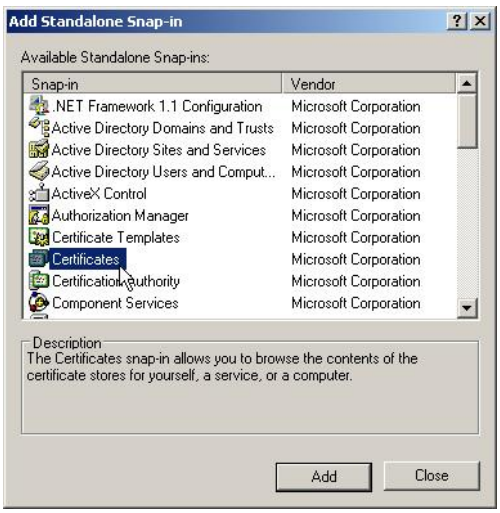
Windows Server 2003 allows the owner of an encrypted file the ability to grant other specific users access to decrypt and view the file. Before a user can be granted access to an encrypted file, that user must have and valid EFS Certificate. In Windows Server 2003, EFS is enabled by default and all users are allowed to encrypt files. When a user encrypts a file for the first time, as described above in Encrypting a file or folder, EFS generates a unique EFS certificate and key pair for the user.

Alternate methods of obtaining an EFS Certificate include importing a certificate into the user's Certificate store, requesting a certificate by using the Advanced Certificate page Web form, or directly requesting an EFS certificate from a CA within the Domain. The procedures below explain how to import an EFS certificate to a Windows Server 2003 stand-alone or member server and how to make a certificate request within a Domain.

Import EFS Certificates

Users can import EFS Certificates as follows:

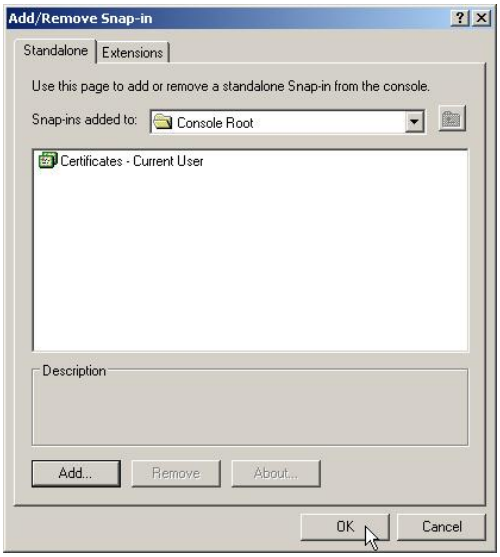
1. Obtain an EFS Certificate from a CA, or from a backup, as necessary.
2. Copy the file to a disk location on the computer where the encryption certificate will be imported.
3. Click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.
4. From the **File** menu, select **Add/Remove snap-ins**, and click **Add**.
5. Locate the **Certificates** snap-in, and click **Add**.



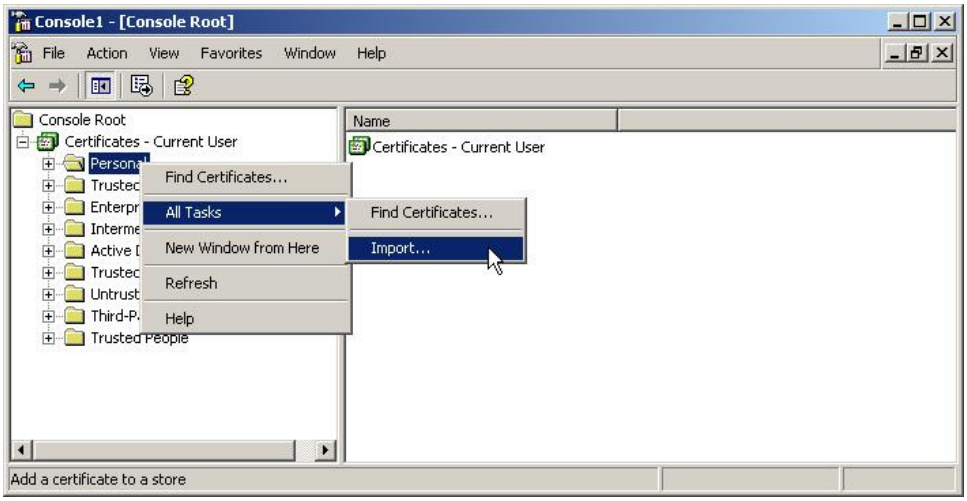
6. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



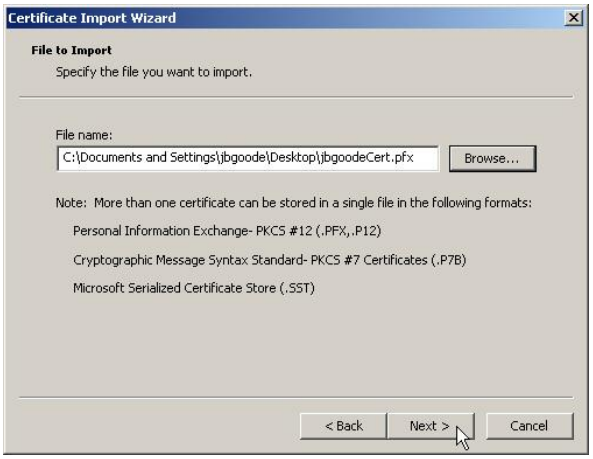
7. Expand the **Certificates – Current User** node under **Console Root**. Right-click **Personal store**, point to **All Tasks**, and select **Import** to import the certificate.



8. This starts the **Certificate Import Wizard**. Follow the wizard steps to successfully import the certificate and private key.

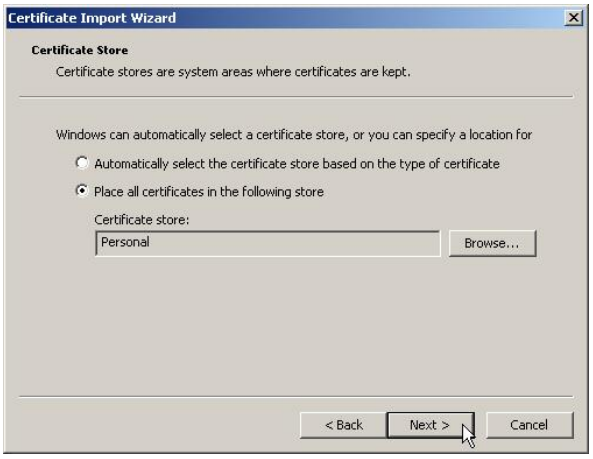
9. Provide the path to the certificate.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



10. If the certificate includes a private key that was protected with a password, a password verification request will appear. Enter the password and check the **Mark this key as exportable** check box in order to allow the ability to back up the keys at a later time. Click the **Next** button.

11. Click the **Place all certificates in the following store** radio button, and accept the **Personal** certificate store. Click **Next**.



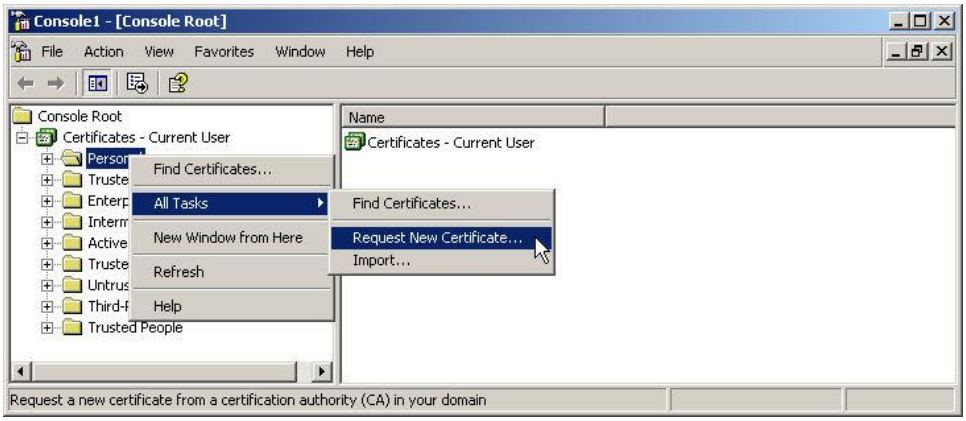
12. Click **Finish**, and then click **OK** to start the import operation. When the import is complete, click **OK** to close the wizard.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Request an EFS Certificate from a CA within a Domain

Users can request an EFS Certificate from a local CA within a Domain as follows:

1. Click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.
2. From the **File** menu, select **Add/Remove snap-ins**, and click **Add**.
3. Locate the **Certificates** snap-in, and click **Add**.
4. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.
5. Expand the **Certificates – Current User** node under **Console Root**. Right-click **Personal store**, click **All Tasks**, and select **Request New Certificate**.



6. This starts the **Certificate Request Wizard**. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

7. In **Certificate Types**, select **Basic EFS**. Click **Next**.

8. Enter a name for the certificate in the **Friendly name** text box. A description may be entered if desired. Click **Next**.

9. Review the request information and click **Finish**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

10. A message will be displayed indicating that the request was received by the CA and is pending action by the Certificate Manager.

11. Once the Certificate Manager approves and issues the certificate, the user will be able to use it to encrypt files locally and on resources, such as share folders, within the Domain.

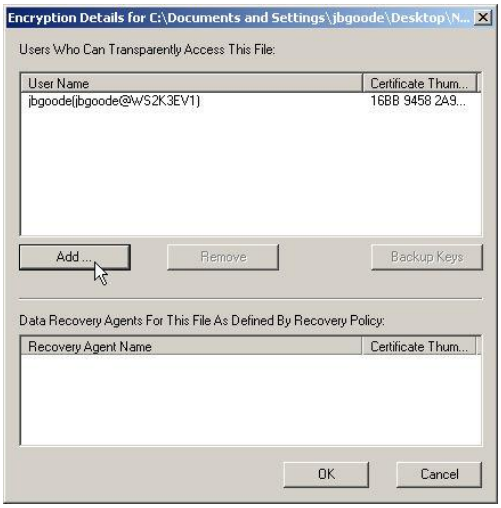
Note: See Appendix B, Windows Server 2003 Certificate Server Evaluated Configuration Administrator's Guide, for procedures a Certificate Manager uses to issue certificate requests.

Granting Local Users Authorization to Open Encrypted Files

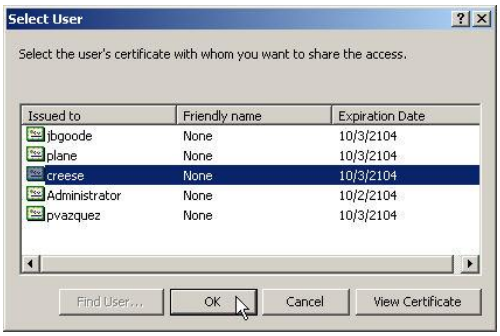
The owner of an encrypted file on a standalone server or domain member server where there is no CA may grant other users the ability to open the encrypted file as follows:

1. Right-click on the encrypted file that is to be shared with other users and click **Properties**.
2. On the **General** tab, click **Advanced**.
3. On the **Advanced Attributes** interface, click the **Details** button. The **Encryption Details for <filename>** interface will appear. Click **Add**.

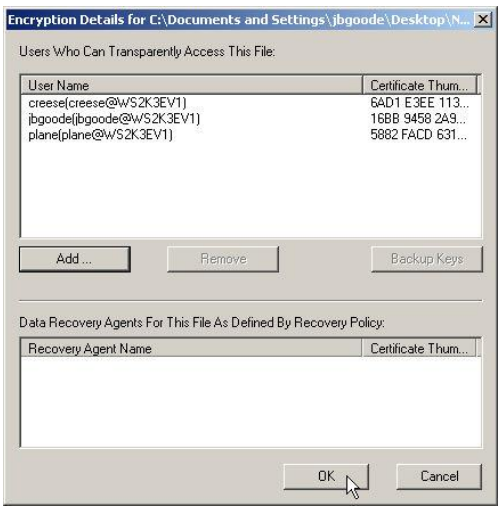
Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. The **Select User** interface will appear. It will display only users that currently have encryption certificates. Select the users to be added and click **OK**.



5. The **Encryption Details for <filename>** interface will display the accounts of all users that are allowed to access the encrypted file. Click **OK** on the **Encryption Details for <filename>** interface, the **Advanced Attributes** interface, and the **Properties** window to close and accept the changes.

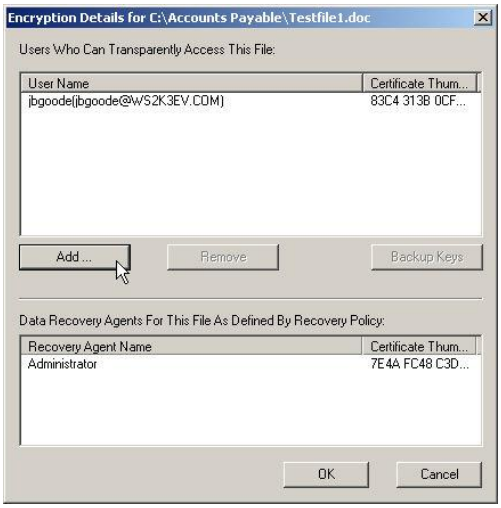


Copyright © 2008 Microsoft Corporation.
All rights reserved.

Granting Domain Users Authorization to Open Encrypted Files

Within a domain that includes a CA, the owner of an encrypted file may grant other users the ability to open the encrypted file as follows:

1. Right-click on the encrypted file that is to be shared with other users and click **Properties**.
2. On the **General** tab, click **Advanced**.
3. On the **Advanced Attributes** interface, click the **Details** button. The **Encryption Details for <filename>** interface will appear. Click **Add**.

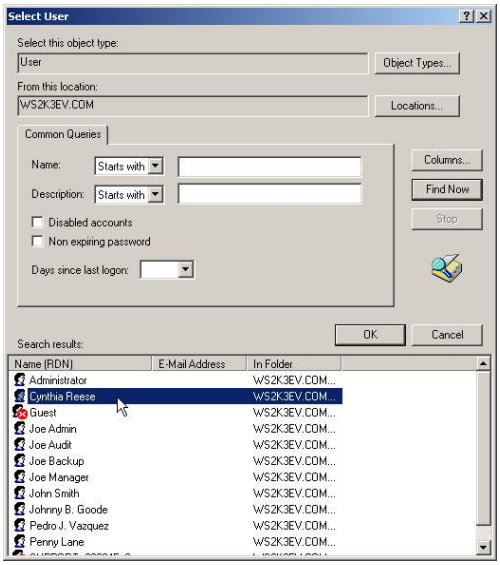


4. On a computer that is a member of a Windows domain, the **Find User** button on the **Select User** dialog widow will be enabled. Click the **Find User** button to search for user accounts on Active Directory.

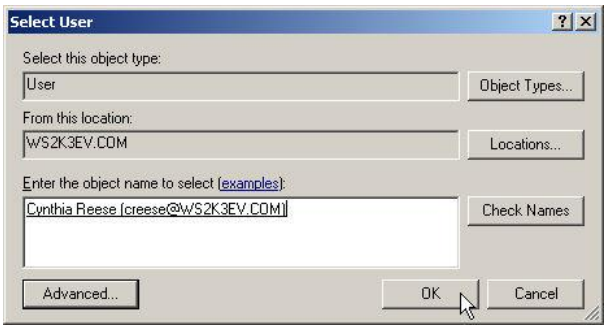
5. Click the **Advanced** button on the next **Select User** dialog widow to open a search window. Click **Find Now** button to display a list of accounts. If necessary, use the **Locations** button to specify a different location from which to select accounts. Select the desired account from the list and click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

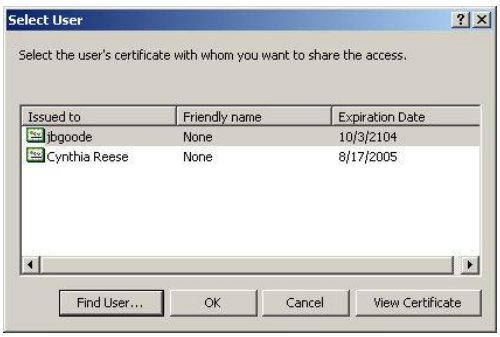


6. Click **OK** again on the **Select User** interface, which shows the selected account.



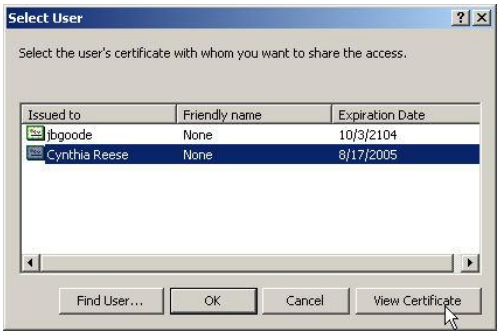
Note: If the user that is selected does not have a valid certificate, a notification will appear stating that **No appropriate certificates correspond to the selected user**. Make sure the user follows the required procedures in "Obtaining EFS Certificates" to obtain a valid certificate. Otherwise, the owner of the encrypted file will not be able to grant access to the user.

7. The account will now appear in the list of certificate holder accounts.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

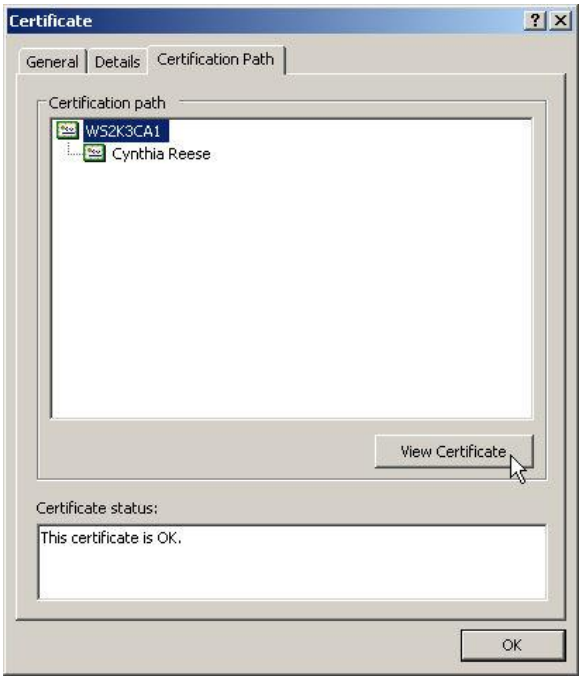
8. If necessary, validate the certificate by selecting the account and clicking the **View Certificate** button. Otherwise, go to step 12.



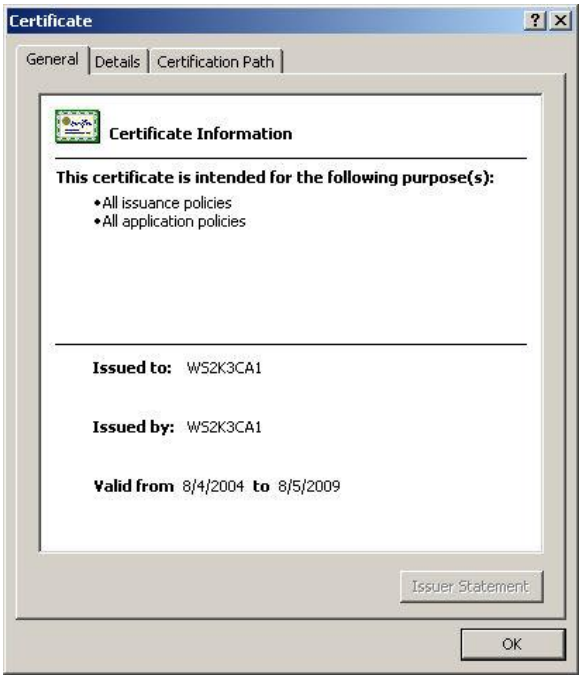
9. The user's certificate will be displayed.

10. To verify the CA for the certificate, click the **Certification Path** tab, highlight the root certificate in the path, and click the **View Certificate** button.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



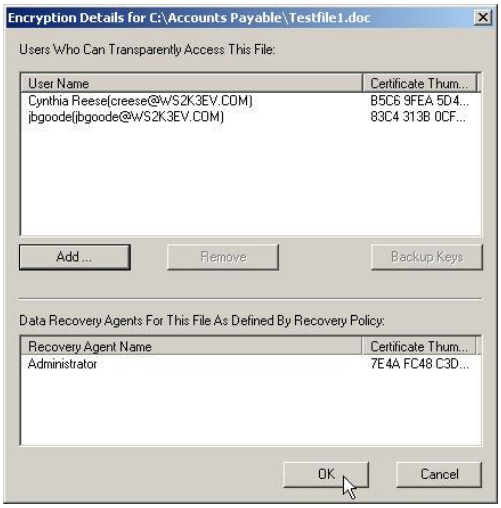
11. The certificate for the root CA will be displayed. Close all certificate windows.



12. Select the desired user from the list presented in the **Select User** interface, and then click the **OK** button.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

13. The user's account will now appear in the list of **Users Who Can Transparently Access This File**. Click **OK** to close the **Encryption Details for <filename>** interface. Click **OK** on the **Advanced Attributes** interface, and the **Properties** window to close and accept the changes.



Revocation Checking

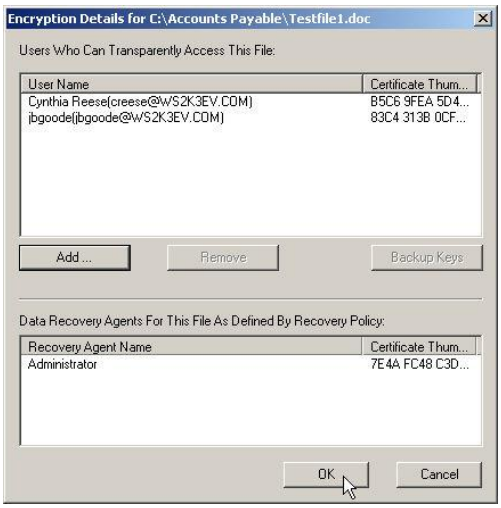
Windows Server 2003 performs revocation checking on all certificates for other users when they're added to an encrypted file. For performance reasons, users that hold a private key and recovery agent certificates are not checked for revocation, they are only verified for time validity. However, user certificates that do not contain a Certificate Revocation List (CRL) Distribution Point (CDP) extension (such as those from some 3rd party CAs) will not be validated for revocation status when added to a file. If the user does not chain to a trusted root CA certificate, or the certificate is not installed in the Trusted People certificate store, the user will be warned before adding the certificate. If the revocation status check on a certificate fails, the message shown below will be displayed and the certificate will not be used.

If the user selects to add a certificate that does not chain to a trusted root CA, it will not be added. However, if the user selects to add a self-signed cert that was installed by another user on the same machine, the user will be allowed to add if they choose **Yes** on the message window below.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

If the revocation status and chain building completed successfully, the user will be added to the interface and the file updated as shown in below. For more information on certificate status and chain building, refer to the following whitepaper:
http://www.microsoft.com/technet/prodtechnol/winxppro/support/tshtcrl.mspx



Notes:

Any user that can decrypt a file can also remove other users if the user doing the decrypting also has write permission.

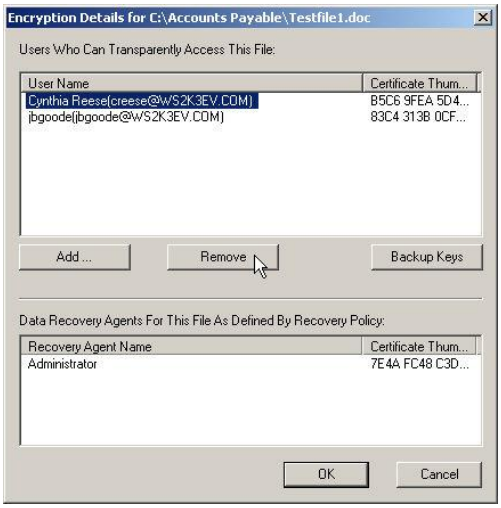
EFS has a limit of 256K in the file header for the EFS metadata. This limits the number of individual entries for file sharing that may be added. On average, a maximum of 800 individual users may be added to an encrypted file.

Removing a User's Authorization to Open an Encrypted File

The owner of an encrypted file may use the following procedure to remove a user's access to the file.

1. Right-click on the one the encrypted file that is to be shared with other users and click **Properties**.
2. On the **General** tab, click **Advanced**.
3. On the **Advanced Attributes** interface, click the **Details** button. The **Encryption Details for <filename>** interface will appear displaying the names of all accounts that have access to the encrypted file. Select the account that is to be removed and click the **Remove** button.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. The account will be immediately removed from the list of authorized accounts. Click **OK** to close the **Encryption Details for <filename>** interface. Click **OK** on the **Advanced Attributes** interface, and the **Properties** window to close and accept the changes.

Decrypting Files and Folders

Encrypted files can only be decrypted using the private key that encrypted them. Decrypt a file as follows:

1. Right-click the folder and click **Properties**.
2. On the **General** tab in the **Properties** interface, click **Advanced**.
3. Clear the **Encrypt contents to secure data** checkbox.

4. Click **OK**.
5. Click **OK** again on the **Properties** window to confirm.

Note: If a folder is being decrypted, there will be an interface offering the option to just decrypt the folder, or to decrypt the folder and all of its contents.

Data Recovery

Data recovery is a process by which individual data elements such as files or folders are encrypted for more than one person or entity. By encrypting for more than one person or escrow entity, multiple paths for data decryption are made available. An escrow entity may be a designated administrator within an

Copyright © 2008 Microsoft Corporation.
All rights reserved.

organization to perform a data recovery role. Data recovery does not necessarily imply that private key recovery has occurred, however, key recovery may be one method to achieve data recovery. Data recovery can be achieved without private key recovery in the Windows Server 2003 OS.

Both Secure Multi-purpose Internet Mail Extensions (S/MIME) and EFS use symmetrically encrypted data blocks, with the symmetric key being protected by one or more public keys of a public/private key pair. In this scenario, the symmetric key may be protected (encrypted) with more than one user, and therefore more than one public key. Data recovery can occur by granting a second user the ability to decrypt the data. In the case of EFS, files can be opened and data recovered through the use of a DRA.

Windows 2000 mandated a requirement that a recovery policy must be in place before users can encrypt files. The recovery policy is a type of public key policy that provides for one or more user accounts to be designated as a DRA. A default recovery policy is automatically put in place for the domain when the domain administrator logs on to the Domain Controller for the first time, making the administrator the recovery agent for the domain. In contrast to Windows 2000, Windows XP Professional and Windows Server 2003 no longer require a recovery policy to be in effect to encrypt files.

The default recovery policy is configured locally for standalone computers. For computers that are part of an Active Directory-based domain, the recovery policy is configured at the site, domain, OU, or individual computer level, and applies to all Windows XP Professional - and Windows Server 2003-based computers within the defined scope of influence. Recovery certificates can be issued by a CA and managed using the MMC Certificates snap-in.

In a network environment, the domain administrator controls how EFS is implemented in the recovery policy for all users and computers in the scope of influence. In a default Windows Server 2003 installation, when the first Domain Controller is set up, the domain administrator is the specified recovery agent for the domain. The way the domain administrator configures the recovery policy determines how EFS is implemented for users on their local machines. To change the recovery policy for the domain, the domain administrator logs on to the first Domain Controller. If a machine is a stand-alone (not joined to a domain), the expiration period of a self-issued administrator account DRA certificate is 100 years. If a machine is joined to a domain, the default DRA certificate issued to the domain administrator has an expiration period of three years.

Administrators can define one of three types of policies:

- **Recovery agent policy**. When an administrator adds one or more recovery agents, a recovery-agent policy is in effect. These agents are responsible for recovering any encrypted data within their scope of administration. This is the most common type of recovery policy.
- **Empty recovery policy**. When an administrator deletes all recovery agents and their public-key certificates, an empty recovery policy is in effect. An empty recovery policy means that no recovery agent exists. The Windows XP Professional or Windows Server 2003 client allows EFS to operate with an empty DRA policy.
- **No recovery policy**. When an administrator deletes the private keys associated with a given recovery policy, a no-recovery policy is in effect. Because no private key is available, there is no way to use a recovery agent and recovery will not be possible.

Although the domain administrator is the default DRA in an Active Directory environment, this capability can be delegated or assigned to one or more users.

Data Recovery on Stand-alone Windows Server 2003

Windows Server 2003 does not create a default DRA on newly installed machines in either a workgroup or in a domain. This effectively prevents previous offline attacks against the administrator account. If a machine is joined to a domain, all users, including local users, inherit the recovery policy form the domain, which includes the domain DRA.

For standalone or workgroup computers, an administrator for each computer needs to manually generate a recovery agent certificate and designate a DRA. Because the computer is stand-alone, EFS creates a

Copyright © 2008 Microsoft Corporation.

All rights reserved.

self-signed certificate for the DRA. The designated DRA can then be added to the computer by using the **Local Security Policy** on the local computer. To manually create a DRA, the **cipher.exe** utility must be used.

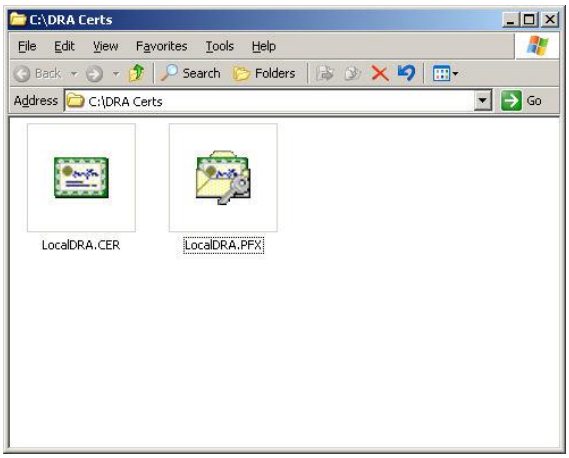
To generate a recovery agent certificate:

1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**. If necessary, change the default directory location to the desired location for the DRA certificates. Make sure the designated DRA has Read and Execute permissions to the folder where the certificates will be created and that the permissions are inherited by files created in the folder. At the command prompt, type the command shown below where filename is the desired name that will be assigned to the certificate.

   Cipher /R:filename
3. After hitting the **Enter** key, a message will appear asking for a password to protect the .PFX file. Enter a password and hit the **Enter** key.
4. A second message will appear asking for confirmation of the password. Reenter the password and hit the **Enter** key.
5. The command will generate *filename*.pfx (Private keys for data recovery) and *filename*.cer (for use in the policy). The following messages will appear.

   Your .CER file was created successfully.

   Your .PFX file was created successfully.



6. Once the keys have been generated the certificate can be imported into the Local Security Policy. Note the location of the files, or move them to a desired location that will be accessible by the individual designated as the DRA. Once the DRA is configured, the files should be removed from the drive and stored in a secure location, such as a safe or locked cabinet. The stored DRA certificates should be used only for emergency file recovery purposes.

To designate a DRA there are two steps; first the user designated as the DRA needs to log on and import the DRA private key into that user's certificate store, then a user with local administrator privileges must add the DRA certificate containing the DRA's public key to the Local Security Policy.

To import the DRA private key:

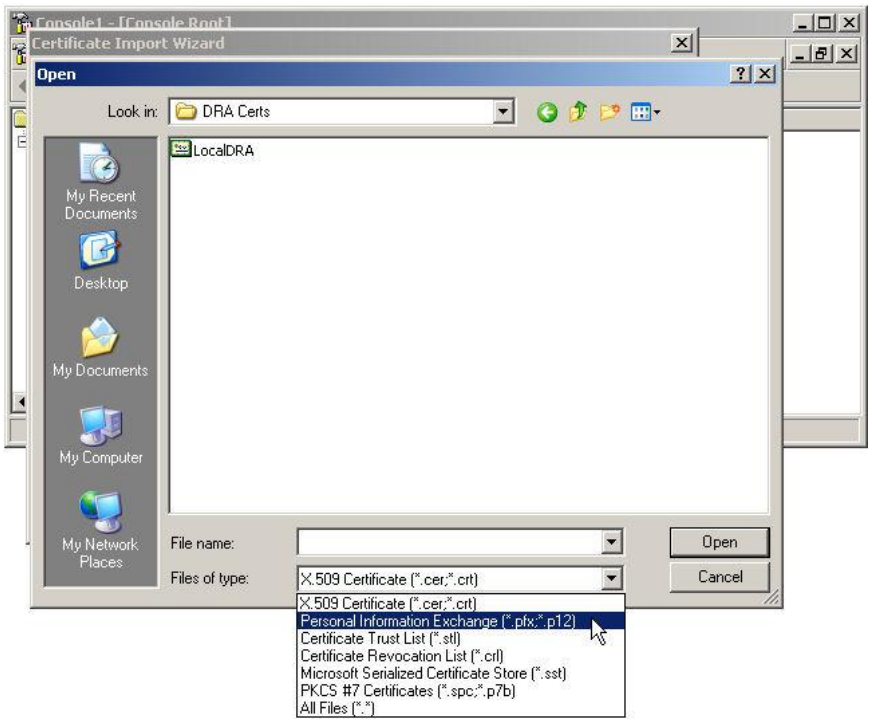
1. The user that has been designated as the DRA must log on to the computer using the account designated for the DRA. In the Evaluated Configuration, the DRA is an authorized administrator role.
2. Click **Start**, click **Run**, type **mmc** in the Open box, and click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

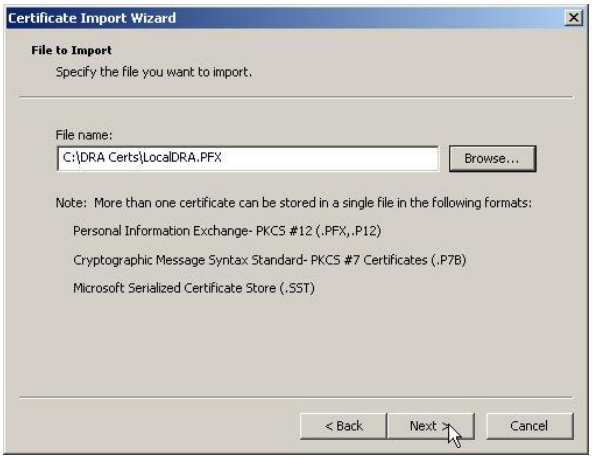
3. On the **File** menu, click **Add/Remove snap-ins**, and click **Add**.
4. Locate and select the **Certificates** snap-in, click **Add**. If the account is a member of the Administrators group, there will be three options available, select **My user account** and then click **Finish**. Click **Close**. Click **OK** on the **Add/Remove snap-in** window. The **Certificates** snap-in will appear in the MMC.
5. Expand **Certificate – Current User**.
6. Right-click **Personal**, point to **All Tasks**, and select **Import**. The **Certificate Import Wizard** will appear. Click **Next**.

7. In the **File to Import** view of the Wizard, click the **Browse** button. In the **Files of type** drop-down menu, select **Personal Information Exchange (*.pfx, p12)**, then select the DRA file and click the **Open** button.



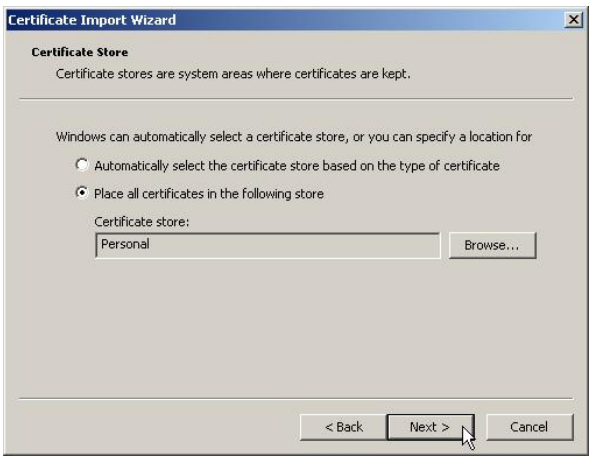
8. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



9. Enter the password that was assigned to the DRA certificate during its creation, check the **Mark this key as exportable** check box, and click **Next**.

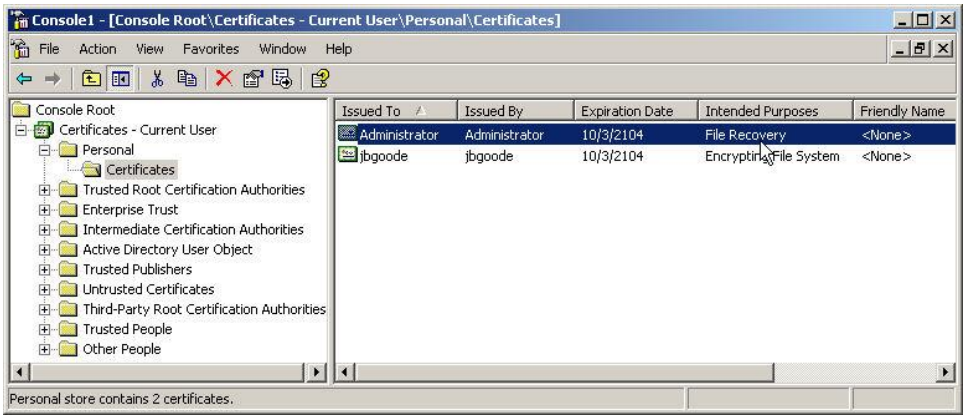
10. Verify that the certificate will be stored in the **Personal** store and click **Next**.



11. Click **Finish** to close the wizard. A message will appear indicating that the import was successful.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

12. Verify that the **Intended Purpose** of the imported certificate indicates that it is for **File Recovery**. As shown below, the user may already have an additional certificate for file encryption.



Note: Although the designated DRA has imported the certificate into his/her certificate store, the DRA certificate will show that it was **Issued to** the administrator that originally created the certificate. This does not prevent the designated DRA from using the certificate.

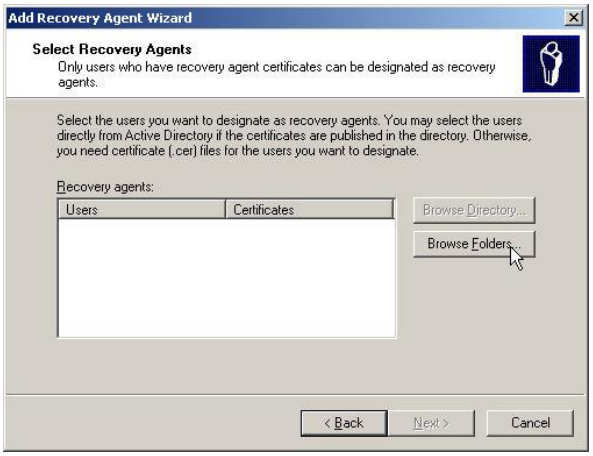
To designate the DRA through the Local Security Policy:

1. Log on as an authorized administrator that is a member of the local Administrators group.
2. Click on **Start**, point to **Administrative Tools**, and then select **Local Security Policy** from the menu. The **Local Security Settings** interface will appear.
3. Expand **Public Key Policies**. Right-click on **Encrypting File System** and select **Add Data Recovery Agent**.

4. The **Add Recovery Agent Wizard** will appear. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

5. Click the **Browse Folders** button to search for the DRA certificate (*.cer).

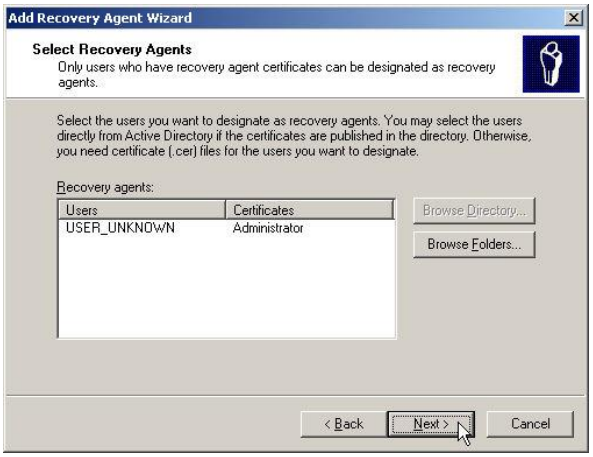


6. Click **Next**. On a stand-alone Windows Server 2003, a message may appear stating that Windows cannot determine if the certificate has been revoked. This is normal since this is a locally created DRA certificate and there is no certificate revocation list (CRL) available.

7. Click **Yes**.

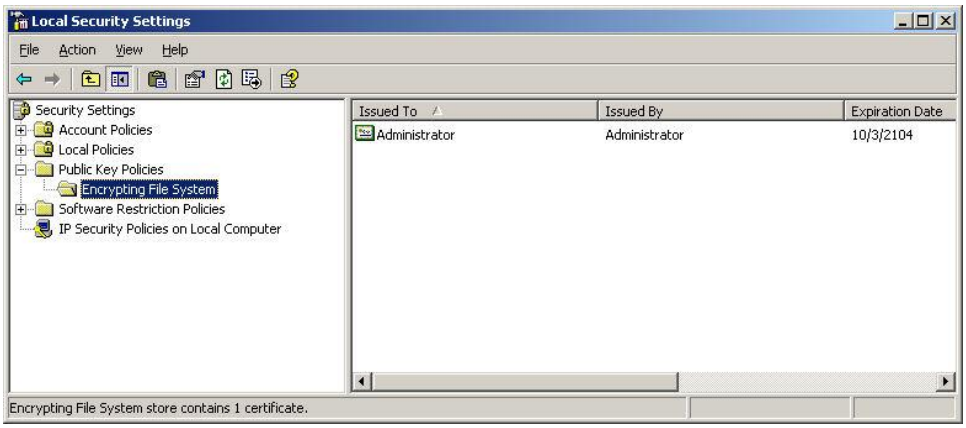
Note: As shown below, under Users, the DRA certificate may state USER_UNKNOWN. This is expected and is not a problem.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



8. Click **Finish**.

9. The DRA certificate containing the public key for the DRA will appear in the **Local Security Policy**. This will allow the certificate to automatically be included with all files encrypted on the local computer.



Data Recovery on Domain Members

As stated earlier, in a Windows domain the Domain Administrator is the default DRA for all domain members. The default DRA for a domain may be changed by the Domain Administrator and assigned to another account that has been designated as the DRA for the domain.

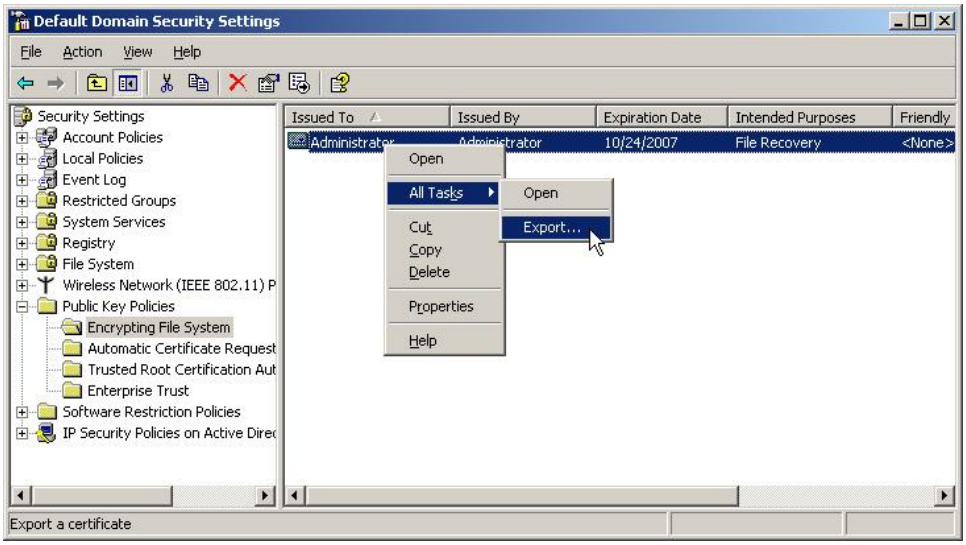
Copyright © 2008 Microsoft Corporation.

All rights reserved.

To recover encrypted data on a computer that is a member of a domain, it is necessary to first export a copy of the DRA file recovery certificate from the Domain Controller, log into the domain member, and import DRA file recovery certificate to the designated DRA's local certificate store. To import the domain DRA certificate, the designated domain DRA must log on locally to the domain member using the DRA domain account, and follow the identical procedures to those explained above for designating a DRA on a standalone computer. Once the DRA file recovery certificate is imported to the local computer, the designated DRA will be able to open the files and recover the data by decrypting them, assigning another user that can decrypt the files, or moving the files as needed. After the recovery, it is recommended that the DRA file recovery certificate, which has the domain DRA's private key be removed from the local computer.

To export a copy of the DRA file recovery certificate from the Domain Controller:

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Domain Security Policy**.
3. Expand **Security Settings** and then expand **Public Key Policies**.
4. Select **Encrypting File System**. In the right-hand details pane, right-click on the domain DRA's certificate, point to **All Tasks**, and select **Export**.



5. Click **Next** on the **Certificate Export Wizard**.

6. Click **Yes, export the private key**. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

7. The export format available is **Personal Information Exchange-PKCS#12**, or .pfx—personal exchange format. **Click Next**.

8. Provide the password to protect the .pfx data. Click **Next**.
9. Provide the path and file name where the .pfx data is to be stored. For this example, type **c:\mykey** in the **File name** entry box. Click **Next**.
10. Review the settings that were specified and click **Finish**.

11. A message will appear indicating that the export was successful. Click **OK** and close the MMC.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

To import the domain DRA certificate to a user's computer, follow the procedures previously described to import the DRA private key.

Copying an Encrypted Folder or File

Because of the unique nature of encrypted files, different results can occur when moving or copying encrypted files between locations. For example, when copying an encrypted file from a local machine to a server on the network, different results of the copy operation will occur depending on the operating system being used on the server. In general, copying a file will inherit the EFS properties of the target, but a move operation will not inherit the EFS properties of the target folder.

The following explains the procedures and limitations for copying encrypted folders or files on the same volume and from one volume to another.

- To copy a file or folder on the same computer from one NTFS partition in a Windows Server 2003 computer to another NTFS partition. Copy the file or folder in the same manner as an unencrypted file. Use Windows Explorer or the command prompt. The copy is encrypted.
- To copy a file or folder on the same computer from an NTFS partition in a Windows Server 2003 volume to a FAT partition. Copy the file or folder in the same manner as an unencrypted file. Use Windows Explorer or the command prompt. Because the destination file system does not support encryption, the copy is not encrypted.
- To copy a file or folder to a different computer where both use the NTFS partitions in Windows XP or Windows Server 2003. Copy the file or folder in the same manner as an unencrypted file. Use Windows Explorer or the command prompt. If the remote computer allows the user encryption of files, the copy is encrypted. When an encrypted file is copied to a target location that does not allow remote encryption, the user will be prompted with an interface that allows a choice of whether or not to decrypt the file. If the target server is running Windows Server 2003, and the machine account of the server is trusted for delegation in the Active Directory, the file will be silently decrypted and copied to the server where it will be re-encrypted using a local profile and encryption key.

Notes:

If the server is a Server Message Block (SMB) file server, the file is transmitted on the network between the client and the server in an unprotected format. If this file contains confidential information, care should be given to ensure that the network connection also provides secure transmission of the data. Such network data protection might include IPSec.

If the server is a WebDav server, it is the encrypted files that travel between WebDav Server and client. In that case, encryption and decryption occurs at the client part of the TOE.

If the original file was encrypted, Microsoft recommends that the status of the destination file be confirmed by looking at the **Advanced Attributes** interface (click the **Advanced** button on the **General** tab of the file's property sheet).

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Moving or Renaming an Encrypted Folder or File

The following explains the procedures and limitations for moving encrypted folders or files on the same volume and from one volume to another.

- **To move or rename a file or folder within the same volume:** Move or rename the file in the same manner as an unencrypted file. Use Windows Explorer, the shortcut menu, or the command prompt. The destination file or folder remains encrypted.
- **To move a file or folder between volumes:** This is essentially a copy operation. Review the previous subsection, Copying an Encrypted Folder or File.

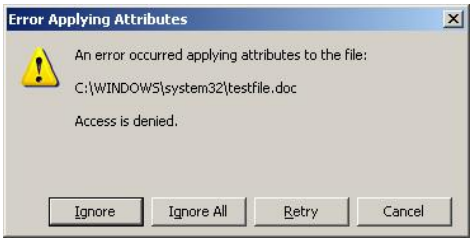
Deleting an Encrypted Folder or File

If a user has sufficient access (e.g., DACLs) to delete the file or folder, the user can delete it in the same manner as an unencrypted file.

Note: Deleting an encrypted folder or file is not restricted to the user who originally encrypted the file.

System Folders and Files

The operating system also prevents encryption of system folders, files and locations in the %SYSTEMROOT%\... path. When a user attempts to encrypt a system file, or attempts to copy an encrypted file into the system path, the user will receive an **Access is denied** message as shown below.



Encryption and Local Account Password Resets on Windows Server 2003

Windows Server 2003 has a new behavior regarding password changes for local accounts and EFS. In Windows 2000, when a local user account password was reset by an administrator, the administrator or third party could theoretically use the newly changed account to log on as the user and decrypt the encrypted files. In Windows XP Professional and Windows Server 2003, the changing of a local user password by an administrator, or through a method other than by the user, will block all access to previously encrypted files by the user.

In summary, the profile and keys of the user will be lost and will not be available to the account with the reset password. Windows Server 2003 gives the following warning when attempting to reset a user account password:

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Clicking Proceed presents the following interface with additional warnings:

This feature helps to guard against offline attacks and prevents rogue administrators from gaining access to encrypted files of other users.

Backing Up an Encrypted Folder or File

The following explains the procedures and limitations for backing up encrypted folders or files.

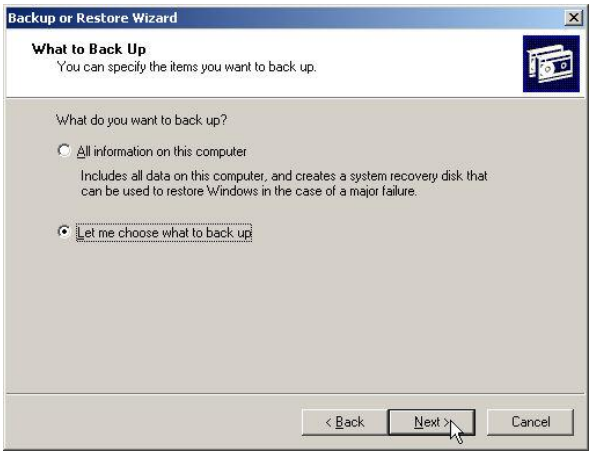
- **Backing up by copying:** A backup created using the **Copy** command or menu selection can end up in clear text, as explained previously in the subsection, Copying an Encrypted Folder or File.
- **Backing up using Backup in Windows Server 2003 or any backup utility that supports Windows Server 2003 features:** This is the recommended way to back up encrypted files. The backup operation maintains the file encryption, and the backup operator does not need access to private keys to do the backup; they only need access to the file or folder to complete the task.

Use **Backup** to back up a file, folder, or drive as follows:

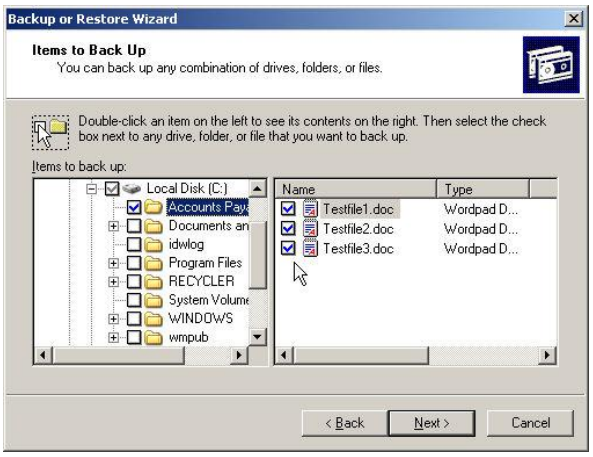
1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then select **Backup**. The **Backup or Restore Wizard** appears. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. Select the **Back up files and settings radio** button and click **Next**.
3. In the **What to Back Up** view of the **Backup or Restore Wizard** choose the types of files that are to be backed up from the set of options. To select specific files, choose **Let me choose what to back** up radio button. Click **Next**.

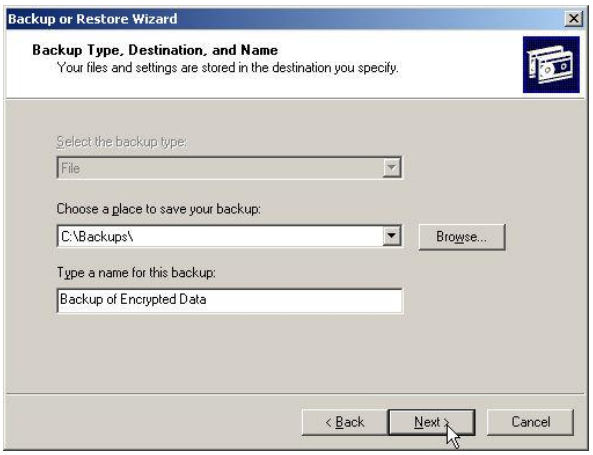


4. Select the drive, files, or folders to back up. (In this example, the **Accounts Payable** folder and selected files).



5. Select the destination for the backup and set the backup file name. Click **Browse** to choose a specific backup location. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



6. Review the information provided in the Wizard for accuracy. Click **Finish** to start the backup process.

7. When the backup process is complete, click **Close** in the **Backup Progress** interface.

The **Backup and Restore Wizard** compresses the entire encrypted file, folder, or drive to the specified backup file. This file can be copied to FAT media, such as floppy disks, and is secure because its contents remain encrypted.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

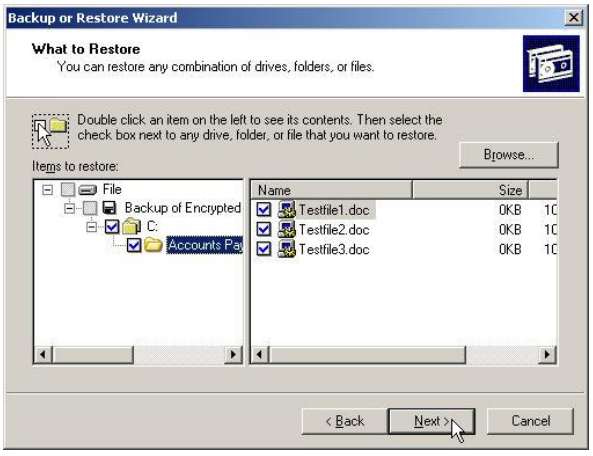
Restoring an Encrypted Folder or File

Restore operations parallel those used for backing up encrypted files. The following explains the procedures and limitations for restoring backed up encrypted files to the computer where the backup was performed and to a computer other than the one where the files were backed up.

- **Restoring by Copying:** Restored files created using the **Copy** command or menu selection can end up in clear text, as explained previously in the subsection Copying an Encrypted Folder or File.
- **Restoring using Backup in Windows Server 2003 or any backup utility that supports Windows Server 2003 features:** This is the recommended way to restore encrypted files. The restore operation maintains the file encryption, and the restoring agent does not need access to private keys to restore the files. After the restoration is complete, the user with the private key can use the file normally.

Use **Backup** to restore a file on the same computer as follows:

1. Either double-click on the backup file, or click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then select **Backup**. The **Backup or Restore Wizard** appears. Click **Next**.
2. Select the **Restore files and settings** radio button and click **Next**.
3. In the **What to Restore** view of the **Backup or Restore Wizard** choose the backup files that are to be restored from the archive. Use the **Browse** button to find specific backup archives. Click **Next**.

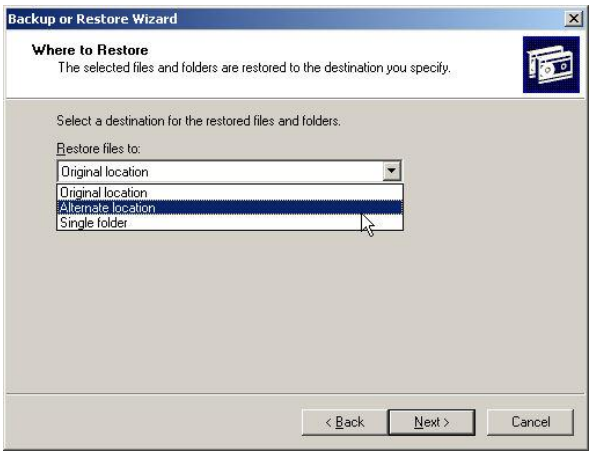


4. Click **Finish** to restore the files to their original location by default, or click **Advanced** to restore the files to an alternate location.

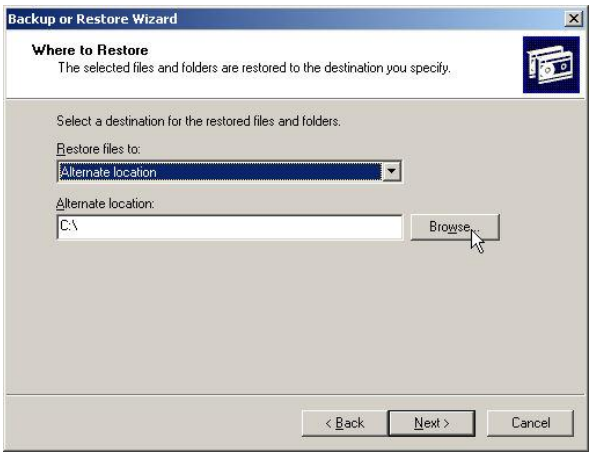
5. If the **Advanced** option was selected, use the **Restore files in** drop-down menu to choose an option.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



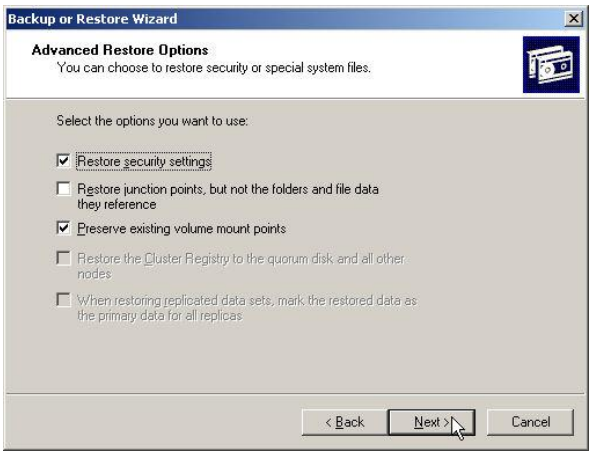
6. Use the **Browse** button to select the location where the files should be restored, then click **Next**.



7. In **the How to Restore** view of the **Backup or Restore Wizard,** choose whether to leave or replace existing files. For this example, choose **Leave existing files (Recommended)** and click **Next**.

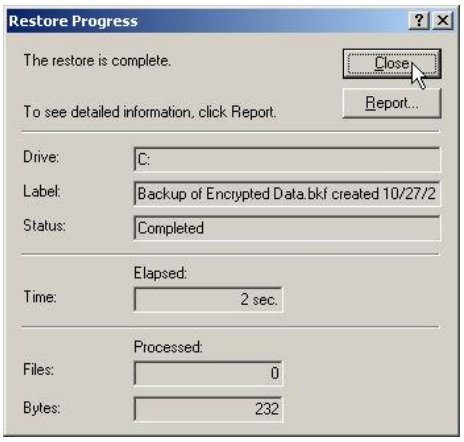
8. In **Advanced Restore Options**, select the defaults and click **Next**. This will preserve the original security settings for the files.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



9. Click **Finish** to restore the files.

10. When the restore process is complete, click **Close**.



The **Restore Progress** dialog shows the progress of the operation. The **Properties** of the folder can be used to check that indeed it was restored encrypted.

Restoring Files to a Different Computer

To be able to use encrypted files on a computer other than the one the files were encrypted on, authorized administrators need to ensure that the encryption certificate and associated private key are available on

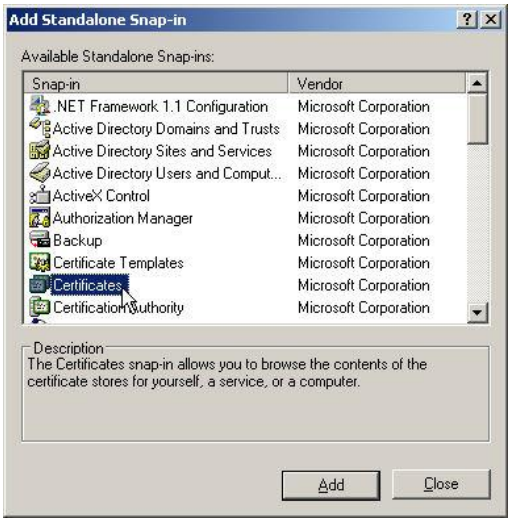
Copyright © 2008 Microsoft Corporation.

All rights reserved.

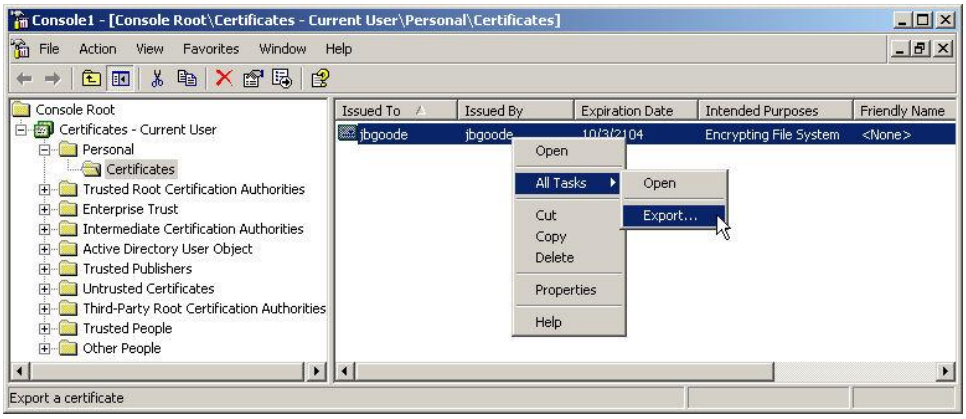
the other system. This can be accomplished by manually moving the keys. Before moving keys manually, authorized users should back up encryption certificates and private keys. They can then restore the certificates and keys on a different system.

Back up the encryption certificate and private key as follows:

1. Log on as the user that is going to export the encryption certificate and private key.
2. Click **Start**, select **Run**, type **mmc** in the **Open** box, and click **OK**.
3. From the **File** menu, select **Add/Remove snap-ins**, and click **Add**.
4. Locate the **Certificates** snap-in, and click **Add**.



5. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.
6. Locate the **Encrypting File System** certificates in the **Personal** certificate store. Click the **+** next to **Certificates–Current User**. Expand the **Personal** folder. Select **Certificates**.
7. Right-click on the user's EFS certificate, point to **All Tasks**, and select **Export**.



8. This starts the **Certificate Export Wizard**. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

9. Click **Yes, export the private key**. Click **Next**.

10. The export format available is **Personal Information Exchange-PKCS#12**, or .pfx—personal exchange format. **Click Next**.

11. Provide the password to protect the .pfx data. Click **Next**.
12. Provide the path and file name where the .pfx data is to be stored. For this example, type **c:\mykey** in the **File name** entry box. Click **Next**.
13. Review the settings that were specified and click **Finish**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

14. A message will appear indicating that the export was successful. Click **OK** and close the MMC.

This exports the encryption certificate and private key to a .pfx file that must be backed up securely.

To restore an encryption certificate and private key on a different system do the following:

1. Copy the .pfx file to a floppy disk, and take it to the computer on which the encryption certificate and private key are to be imported.
2. Log on to the other computer as the user that owns the encryption certificate and private key.
3. Click **Start**, select **Run**, type **mmc** in the **Open** box, and click **OK**.
4. From the **File** menu, select **Add/Remove snap-ins**, and click **Add**.
5. Locate the **Certificates** snap-in, and click **Add**.
6. Select **My user account** and then click **Finish**. Click **Close**. Click **OK**.
7. Right-click **Personal** store, point to **All Tasks**, and select **Import** to import the .pfx file.

8. This starts the **Certificate Import Wizard**. Click **Next** and follow the wizard steps to successfully import the certificate and private key.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

9. Provide the path to the .pfx file. In our example, it is **c:\mykey.pfx**. If necessary, use the **Browse** button to search for the file. The **Type of file** selection for the search is **Personal Information Exchange (*.pfx, *.p12)**. Click **Next**.

10. Type the password to unwrap the .pfx data. Click **Next**.

11. Select the **Place all certificates in the following store** radio button, and accept the **Personal** certificate store. Click **Next**.

12. Review the settings and click **Finish** to close the wizard.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

13. A message will appear indicating that the import was successful. Click **OK** and close the MMC.

Once the same user's EFS keys are available on the second computer, the user can transparently use encrypted files that may have been backed up on a different computer.

Folder and File Encryption on a Remote Server

Users can transparently encrypt and decrypt files and use encrypted files stored on a remote server. This works whether the users access those files remotely or log on to the other computer locally. However, remember that when encrypted files are moved using backup and restore mechanisms, the appropriate encryption certificate and private keys must also be moved to allow use of the encrypted files in their new destinations. Without correct private keys, users cannot open or decrypt the files.

> **Note:** If an encrypted file is opened over the network, the data that is transmitted over the network by this process is not encrypted. Other protocols, such as SSL/Personal Communication Technology (SSL/PCT) or IPSec, or WebDAV must be used to encrypt data over the wire.

Remote EFS Operations in a Web Folder Environment

When users open encrypted files stored on Web folders, the files remain encrypted during the file transfer, and EFS decrypts them locally. Both uploads to and downloads from Web folders are raw data transfers, so even if an attacker could access the data during the transmission of an encrypted file, the captured data would be encrypted and unusable.

Using EFS with Web folders eliminates the need for specialized software to securely share encrypted files between users, businesses, or organizations. Files can be stored on common intranet or Internet file servers for easy access while strong security is maintained by EFS.

The WebDAV redirector is a mini-redirector that supports the WebDAV protocol, an extension to the HTTP 1.1 standard, for remote document sharing over HTTP. The WebDAV redirector supports the use of existing applications, and it allows file sharing across the Internet (for example, using firewalls, routers) to HTTP servers. IIS versions 5.0 (Windows 2000) and 6.0 (Windows Server 2003) support Web folders.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Users access Web folders in the same way that they access file shares. Users can map a network drive to a Web folder by using the net use command or by using My Computer. Upon connecting to the Web folder, the user can choose to copy, encrypt, or decrypt files exactly as they would by using files on file shares. See the Web Distributed Authoring and Versioning (WebDAV) subsection for details on using WebDav.

Audit Management

Windows events and Performance Logs and Alerts are recorded by the Event Log service. The Event Log service starts automatically when Windows Server 2003 is started. All users can view the Application and System logs; however, only administrators have access to the Security logs.

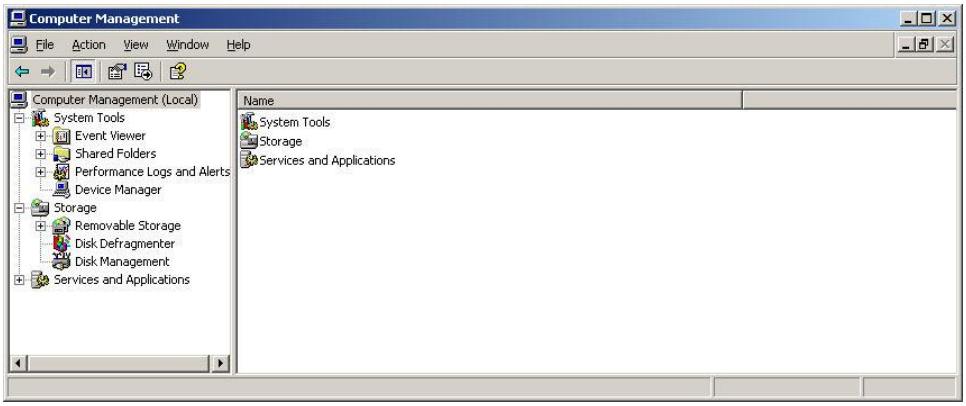
By default, security logging is turned on for Windows Server 2003. Use Group Policy, as described in the Configuring Audit Policies subsection of this document, to modify audit settings. An authorized administrator can also set auditing policies in the registry that cause the system to halt when the security log is full. Procedures for this are provided under Shut Down System Immediately If Unable to Log Security Audits subsection of this document. In addition, Appendix B, Audit Categories and Events, of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* provides a cross reference of audit categories and audit events to the auditable events addressed by the Windows 2003/XP V3 ST requirements.

The Event Viewer **Security** log displays the following types of events:

- **Success audit**. An audited security access attempt that succeeds. For example, the successful attempt by a user to log on the system will be logged as a success audit event.
- **Failure audit.** An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a failure audit event.

Viewing the Security Log

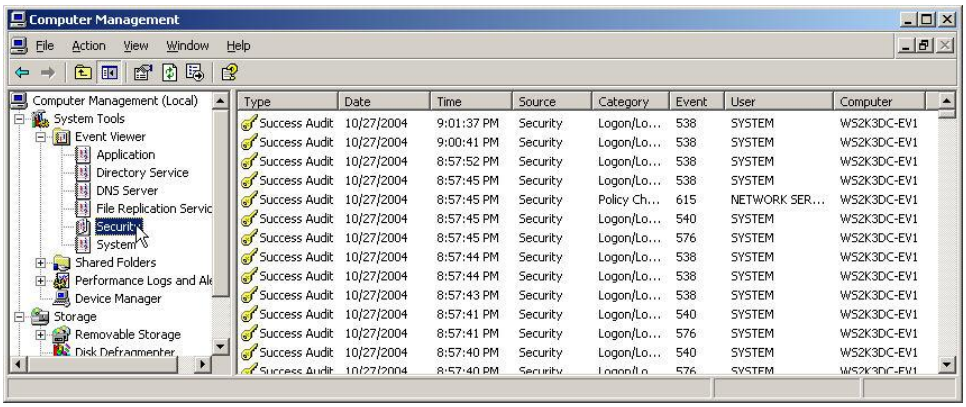
1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Computer Management**.



3. In the console tree, expand **Event Viewer**. Select **Security** and in the details pane, examine the list of audit events.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

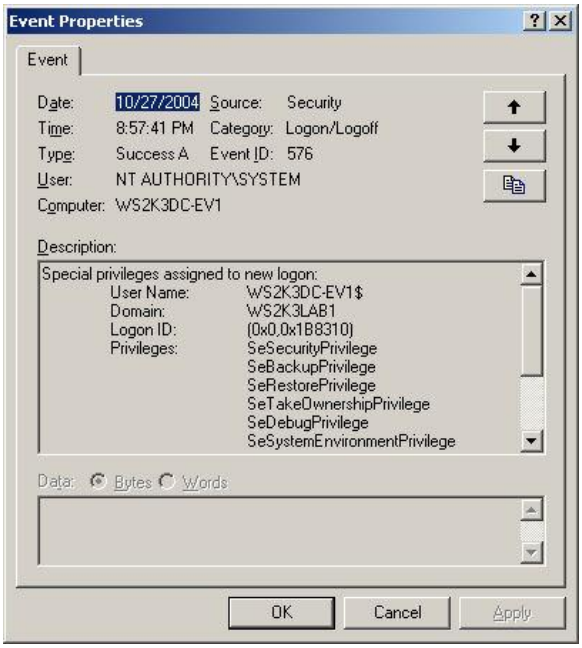


4. Scroll through the details pane to view the various fields. The event fields are described below.

Event field	Description
Type	The event logs record five types of events: ▪ Error - A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged. ▪ Warning - An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged. ▪ Information - An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged. ▪ Success Audit - An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event. ▪ Failure Audit - An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
Date	The date the event took place.
Time	The time the event took place.
Source	The process that raised the event.
Category	The specific class the event is categorized under.
Event	A unique numerical identifier for the event.
User	The user that generated the event.
Computer	The computer on which the event was generated.

5. Event details provide more information about events than the Events view. This additional information includes the event's source, a description of the event, and details about what is affected by the event. To view additional details for an event, double-click on the event. An event **Properties** window will appear.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

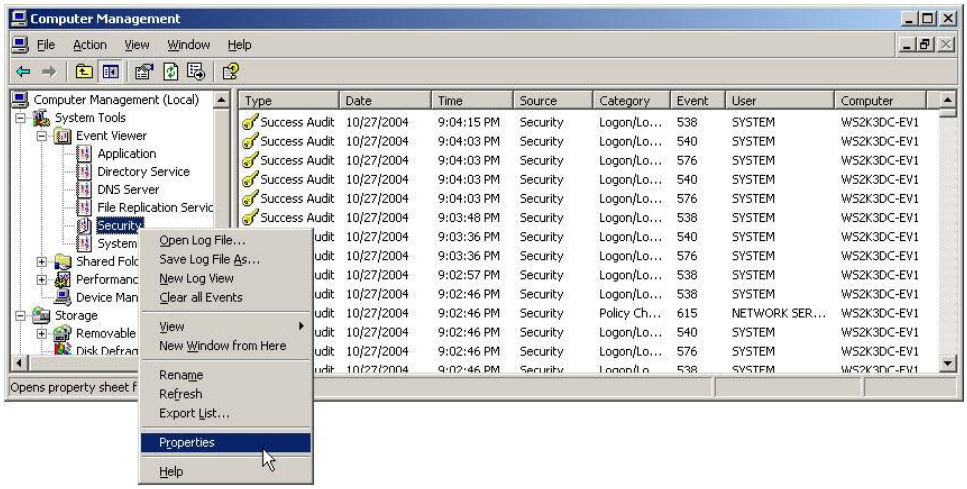


6. The **Description** field of the event **Properties** window provides a longer explanation for the event, including what resources are affected and other technical information.
7. Appendix B of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* provides additional descriptions of Windows Server 2003 security events that can be used in defining the information presented in the event logs.

Configuring the Event Logs

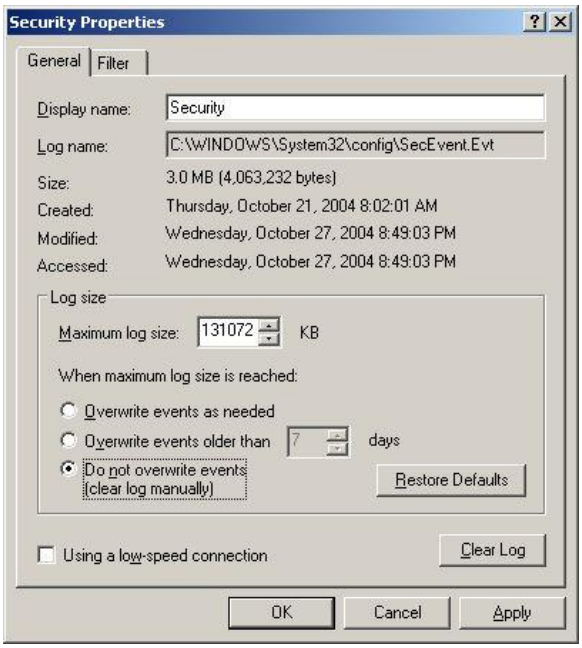
Authorized administrators can define security settings for the event logs. The choices include log size, the length of time a log should be stored, and when the log should be cleared. Each event log can be configured individually.

1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Computer Management**.
3. In the console tree, expand **Event Viewer**. Right-click **Security** and select **Properties**.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

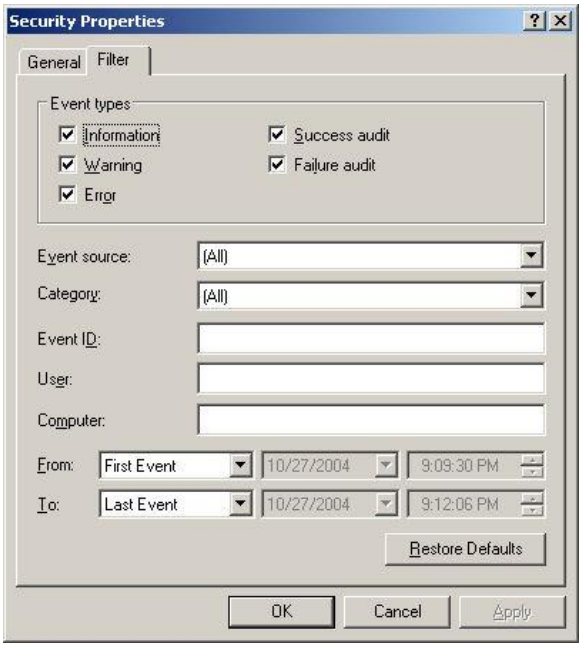
4. The **Security Properties** interface will appear. From this interface, authorized administrators can set the **Maximum log size** and select what action to take when the maximum log size is reached.



- To restore the default settings, click **Restore Defaults**.
- To clear the log, click **Clear Log**.
- Under **Log size**, select one of these options:
  - If the log is not to be archived, click **Overwrite events as needed**.
  - To archive the log at scheduled intervals, click **Overwrite events older than** and specify the appropriate number of days. Be sure that the **Maximum log size** is large enough to accommodate the interval.
  - To retain all the events in the log, click **Do not overwrite events (clear log manually)**. This option requires that logs be cleared manually. When the maximum log size is reached, new events are discarded. This results in a loss of audit information, which is why regular audit maintenance (reviewing, archiving, and clearing the logs) is critical. If the event log is not cleared and archived regularly, a message will appear on the **Log On to Windows** interface stating that the security log is full and only administrators can fix the problem.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

5. After establishing the security log settings, click the **Apply** button.
6. The **Security Properties** interface also provides the ability to set filters on the event log to perform searches and sorting of audit data. To filter an existing event log in order to view or save specific security events, select the **Filter** tab and configure the filter. The filter interface can also be accessed by right-clicking the **Security** log in the console tree, pointing to **View**, and selecting **Filter**.



7. To configure the filter, select the **Event types** that will be included by checking or unchecking a selection box next to **Information**, **Warning**, **Error**, **Success Audit**, and/or **Failure audit**, then input any additional desired filtering requirements by **Event source**, **Category**, **Event ID**, **User**, or **Computer**. Descriptions of these selection options are provided in the previous subsection "Viewing the security log."
8. By default, the entire event log will be filtered for viewing by the parameters selected above. If desired, select a date and time range for the logs that will be filtered for viewing. This is accomplished by first clicking on the **From:** drop down menu and changing the selection to **Events On**. The date and time interfaces will become active. Change the date by selecting the drop down menu and choosing a date from the calendar that is presented. Change the time by scrolling the up and down

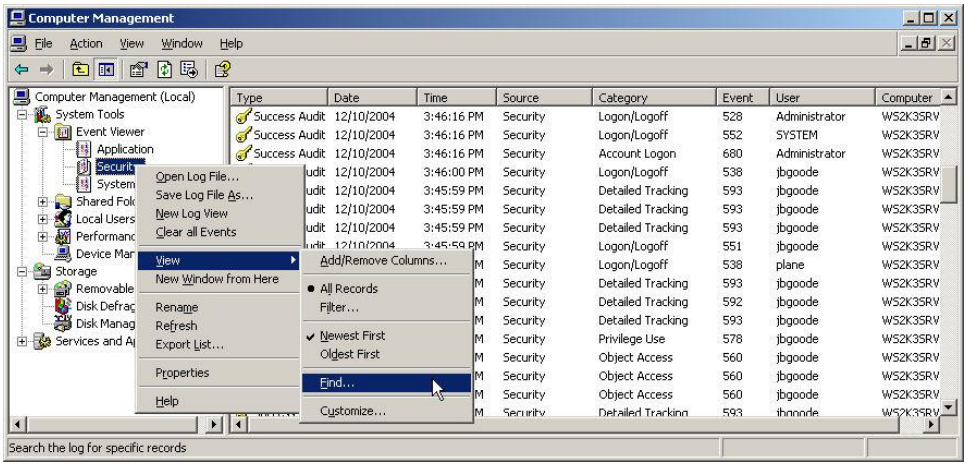
Copyright © 2008 Microsoft Corporation.
All rights reserved.

arrows in the time interface. Follow the same procedures clicking on the **To:** drop down menu and changing the selection to **Events On**. Set the date and time for the last as described above.

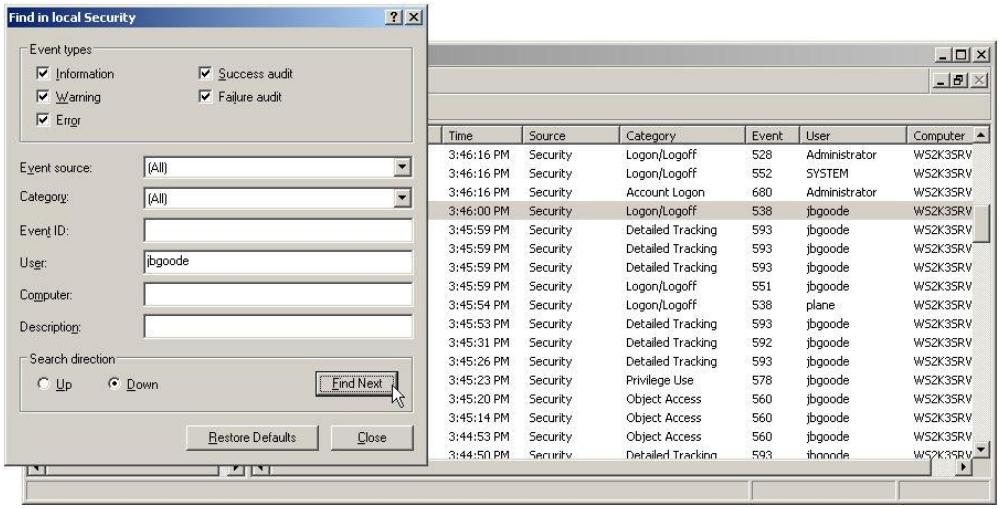
9. Once all the desired filtering options have been selected, click the **Apply** button and click **OK**. The **Event Viewer** will filter the log and display the information as defined by the filter.

Searching for Specific Events

1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Computer Management**.
3. In the console tree, expand **Event Viewer**. Right-click **Security** (or other event log), point to **View**, and select **Find**.



4. The **Find in local Security** interface will appear. Under **Event types**, specify the types of events for which to search. In **Event source**, **Category**, **Event ID**, **User**, **Computer**, or **Description**, specify additional information, as needed, to further define the search.



5. Click the **Find Next** button. This will find and highlight the first event matching the search criteria. Clicking the **Find Next** button again will find the next matching event. This can be done continuously to search through the entire log for each matching event.

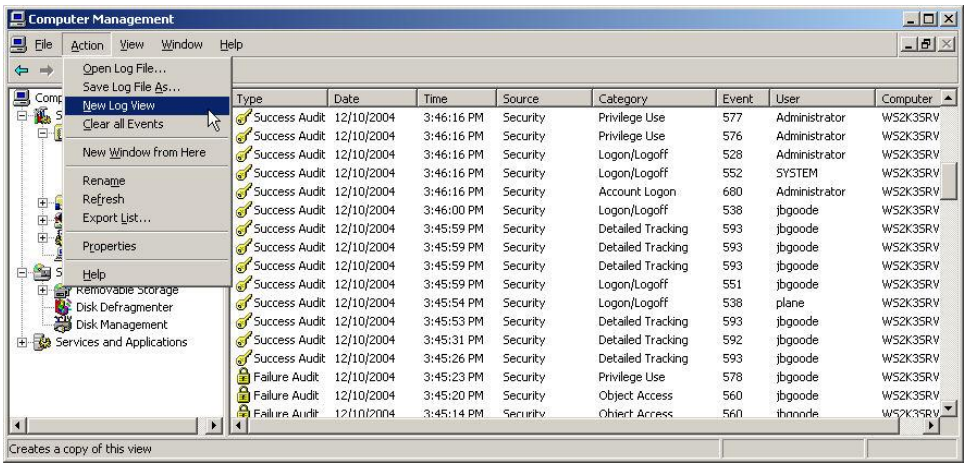
Copyright © 2008 Microsoft Corporation.

All rights reserved.

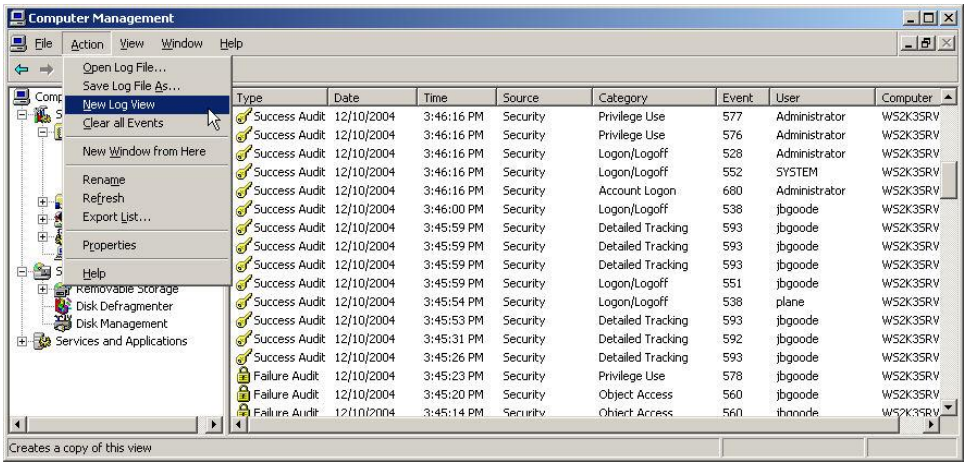
Adding another View of an Event Log

By creating a new log view, authorized administrators can customize how Event Viewer displays the information of an existing log and then apply a new name to the new log view, while keeping the defaults or the options set for the original log intact. Log views added to the console tree can be managed and customized in the same way as the default logs.

1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Computer Management**.
3. In the console tree, expand **Event Viewer**. Select the event log for which a new view is desired.
4. From the **Action** menu, select **New Log View**.



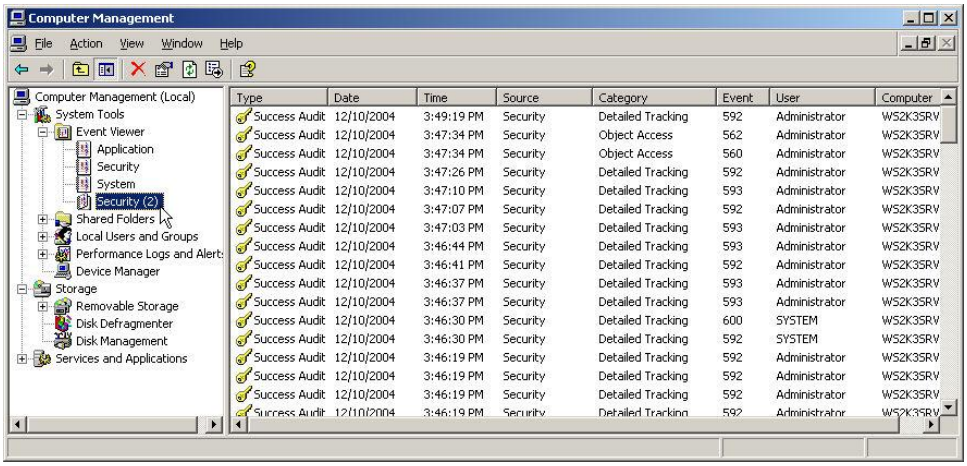
5. A copy of the log appears in the console tree with a default name. For example, if the **Security** log was selected, the default name of the copy would be **Security (2)**.



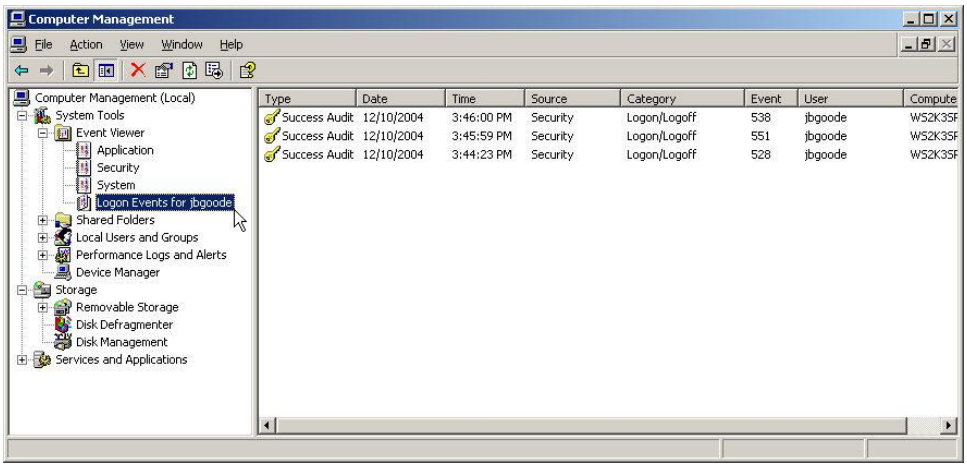
6. To change the name of the log copy, highlight the log copy and select **Rename** from the **Action** menu. Type a new name for the log, as shown in the example below.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



7. The new log view can now be filtered and managed as desired without impacting the original log view. For the example below, a filter was set to only show all **Logon/Logoff** events for account **jbgoode** in the new log view.



Note: If the **New Log View** is created using the **Event Viewer** or **Computer Management** interfaces from the **Administrative Tools** menu, the new view will not be permanent. Once the **Event Viewer** is closed, the **New Log View** will need to be recreated if needed. To make a static **New Log View** that will always be available, use the **MMC** with the **Event Viewer snapin**, create the **New Log View** with the desired filtering, then save the **MMC** snapin. The saved snapin will retain the **New Log View** settings.

Per-User Selective Audit

Starting with SP1 for Windows Server 2003, and SP2 for Windows XP Professional, a new tool called **auditusr.exe** was introduced, which allows authorized administrators to set audit policy exceptions on a per-user basis. This capability is known as "***Per-User Selective Audit***."

Per-User Selective Audit can only be set on individual user accounts. It cannot be used to selectively audit group accounts. Additionally, **Per-User Selective Audit** will not exclude user accounts that are members of the Administrators group. Any attempt to set **Per-User Selective Audit** for an account belonging to the Administrators group will be ignored.

The table below defines the command options that may be used with auditusr.exe and the audit categories that may be specified.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Auditusr.exe Command Options	Valid Categories
/?	Account Logon
Prints command-line help. If no parameters are given then the current settings will be displayed.	Account Management
/is <security principal>:<list of comma-delimited categories>	
Adds or changes an include-success entry	Detailed Tracking
/if <security principal>:<list of comma-delimited categories>	
Adds or changes an include-failure entry	Directory Service Access
/es <security principal>:<list of comma-delimited categories>	
Adds or changes an exclude-success entry	Logon/Logoff
/ef <security principal>:<list of comma-delimited categories>	
Adds or changes an exclude-failure entry	Object Access
/r <security principal>	Policy Change
Removes all per-user auditing entries for that security principal	
/ra	Privilege Use
Removes all per-user auditing entries	
/e <filename>	System Event
Exports current per-user auditing settings to a file	
/i <filename>	
Imports current per-user auditing settings from a file	

There are some peculiarities about using the standard audit policy that must be understood in order to use the auditusr.exe utility effectively:

- For any success or failure inclusion entry that is required, the audit categories being specified in the auditusr command must first be set to not audited. The auditusr setting will then add (include) only the account that is specified.
- For any success or failure exclusion entry that is required, the audit categories being specified in the auditusr command must first be set in the audit policy. This will set the audit category for all users, the auditusr setting will then exclude only the account that is specified from being audited.

For example:

To audit successful "Privilege Use" and "Policy Change" events ***only for the jbgoode user account***, first open the security policy, and make sure that the successful events for "Privilege Use" and "Policy Change" in the Audit Policy are not being audited:

1. Log on as an authorized administrator.
2. Open the appropriate security policy (Local or Domain-Level).
3. Expand **Local Policies** and select **Audit Policy**. Double-click on **Audit policy change** policy and clear the **Success** check box. Click **OK**.
4. Repeat the procedures to clear the **Success** check box in the **Audit privilege use** policy.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

5. Open a command line interface and execute the "**gpupdate /force**" command to update the security policy.
6. To set per-user auditing to audit successful "Privilege Use" and "Policy Change" events for account jbgoode, open a command line interface and execute the following command:

   auditusr /is jbgoode:"privilege use", "policy change"

   Note: In order for the command to work, audit categories that have two words with a space between them must be enclosed in quotation marks.

7. As a result of the previous actions, the only user account that will be audited for successful "Privilege Use" and "Policy Change" actions will be the jbgoode user account. Only privilege use and policy change actions performed by jbgoode will appear in the **Security** log. Privilege use and policy change actions by all other users will not appear in the **Security** log.

To audit successful "Privilege Use" and "Policy Change" events for all user accounts ***except the jbgoode user account***, first open the security policy, and make sure that the successful events for "Privilege Use" and "Policy Change" in the Audit Policy are being audited:

1. Log on as an authorized administrator.
2. Open the appropriate security policy (Local or Domain-Level).
3. Expand **Local Policies** and select **Audit Policy**. Double-click on **Audit policy change** policy and select the **Success** check box. Click **OK**.
4. Repeat the procedures to select the **Success** check box in the **Audit privilege use** policy.
5. Open a command line interface and execute the "**gpupdate /force**" command to update the security policy.
6. To set per-user auditing to exclude audit successful "Privilege Use" and "Policy Change" events for account jbgoode, open a command line interface and execute the following command:

   auditusr /es jbgoode:"privilege use", "policy change"

7. As a result of the previous actions, the only user account that will not be audited for successful "Privilege Use" and "Policy Change" actions will be the jbgoode user account. Privilege use and policy change actions performed by jbgoode will not appear in the **Security** log. Privilege use and policy change actions by all other users account will appear in the **Security** log.

Archiving an Event Log

To archive an event log, use the following procedures:

1. Open **Event Viewer** as described in the previous subsection.
2. In the console tree, click the log that is to be archived.
3. On the **Action** menu, click **Save Log File As**. A **Save <*logname*> As** window will appear.
4. In the **File name:** interface, enter a name for the archived log file.
5. In the **Save as type:** drop down menu, select a file format.
   - If the log is archived in log-file format, it can be reopened it in Event Viewer. Logs saved as event log files (*.evt) retain the binary data for each event recorded.
   - If the log is archived in text or comma-delimited format (*.txt and *.csv, respectively), it can reopened in other programs such as word processing or spreadsheet programs. Logs saved in text or comma-delimited format do not retain the binary data.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

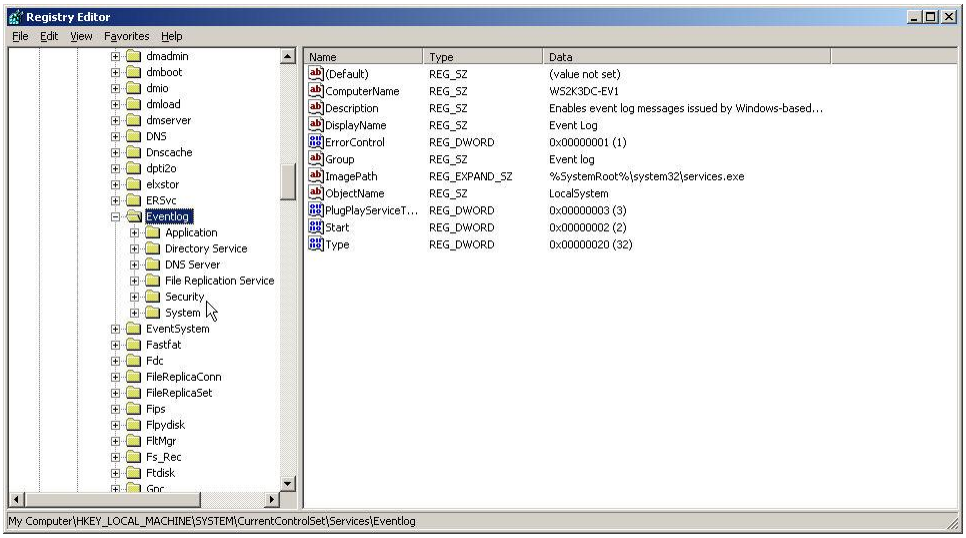
6. If the file is to be saved in a location other than the default, use the **Save in** drop down menu to save the audit log in an alternate location.
7. Click **Save**.
8. After the log has been archived, the original may be deleted by clearing the log as described in the Configuring the Event Log subsection. This will free up disk space and reinitiate the event log.

Change the Default Event Viewer Log File Location

If there is insufficient disk space, the **Event Viewer** may not be able to write event messages to any of the log files. To increase the disk space that can be used for these log files, the default location can be changed in order to relocate the files to a larger disk or partition. To modify the location of the Event Viewer log files:

Warning: Using Registry Editor incorrectly can cause serious, system-wide problems that may require reinstallation of Windows Server 2003 to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved.

1. Click **Start**, Select **Run**, type **regedit**, and then click **OK** to open the Registry Editor.
2. Navigate the Registry tree to **HKEY_LOCAL_MACHINE\CurrentControlSet\Services\EventLog**. As shown, the subkeys under \EventLog include **\Application**, **\Security**, and **\System**.



- For the Application log:
  - Select the \Application subkey folder, and then double-click the **File** value.
  - Type the new drive and path in the **String** box, include the file name \AppEvent.Evt, and then click **OK**. The default path is %SystemRoot%\System32\Config\AppEvent.Evt.
- For the Security log:
  - Select the \Security subkey folder, and then double-click the **File** value.
  - Type the new drive and path in the **String** box, include the file name \SecEvent.Evt, and then click **OK**. The default path is %SystemRoot%\System32\Config\SecEvent.Evt.
- For the System log:
  - Select the \System subkey folder, and then double-click the **File** value.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Type the new drive and path in the String box, include the file name \SysEvent.Evt, and then click **OK**. The default path is %SystemRoot%\System32\Config\SysEvent.Evt.

3. Exit the **Registry Editor** by selecting **Exit** from the **File** menu, and then restart the computer for the settings to take effect.

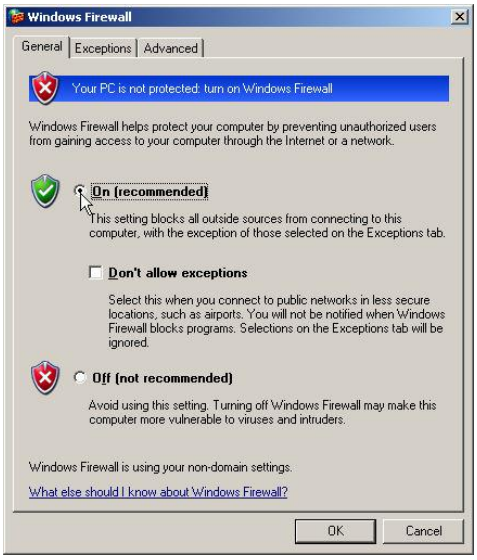
Windows Firewall Configuration and Management

Windows Firewall is a stateful filtering firewall for Windows Server 2003. It provides protection for PCs connected to a network by rejecting unsolicited inbound connections through TCP/IP version 4 (IPv4). Starting with Windows Server 2003 SP1 the IP version 6 (IPv6) was added to the Windows Firewall and automatically enabled on all IPv6 connections. Both IPv4 and IPv6 share the same settings for excepted traffic.

Note: For the Evaluated Configuration, IPv6 must not be used if IPSec is to be enabled. This is due to the limitations of IPv6 in supporting IPSec functions. See notes in the Administering IPSec subsection.

In Windows Server 2003, the Windows Firewall is disabled by default. When enabled, it will start during the boot process. The firewall driver has a static rule, called the **boot-time policy** that performs stateful filtering and eliminates the window of vulnerability while the computer is booting. The **boot-time policy** configuration cannot be modified.

The **run-time Windows Firewall policy** can be modified using the **Windows Firewall** interface shown below. The **run-time Windows Firewall policy** allows all traffic for network connections initiated locally and blocks all unsolicited external network connection attempts except for those that are defined in the policy as exceptions.



Windows Firewall Features

The Windows Firewall in Windows Server 2003 with SP2 includes a number of features to protect the local system from external attacks and to provide administrators with added configuration capabilities needed to meet operational requirements for specific network environments. The Windows Firewall in Windows Server 2003 with SP2 includes the following features:

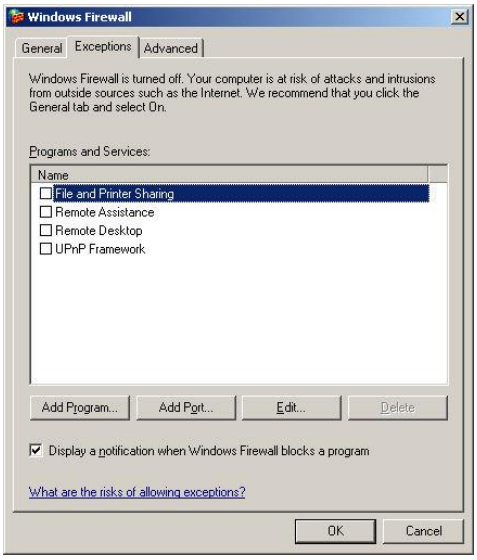
- The firewall is enabled by default for all of the connections of the computer

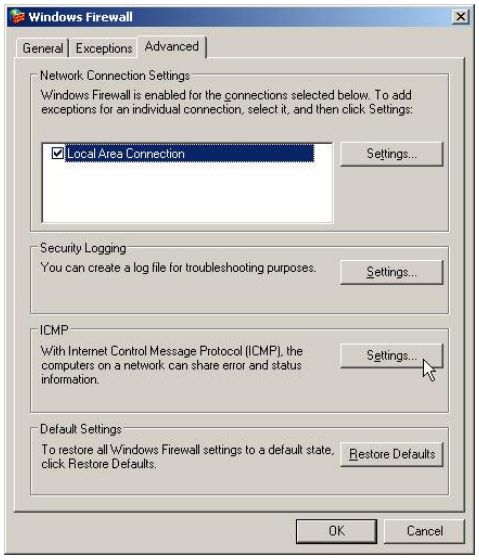
Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Global configuration options that apply to all connections
- Connection specific configuration options
- Operating mode options for excepted traffic
- Startup security
- Incoming traffic scoping for IPv4
- Built-in support for IPv6
- Excepted traffic can be specified by program filename
- Configuration using group policy settings

Global Configuration Options

Windows Firewall in Windows Server 2003 with SP2 allows the configuration of firewall settings that apply to all the connections of the computer (global configuration). When a global Windows Firewall setting is changed, the change is applied to all the connections on which Windows Firewall is enabled. Global configuration options are available on all tabs in of the **Windows Firewall** management interface.



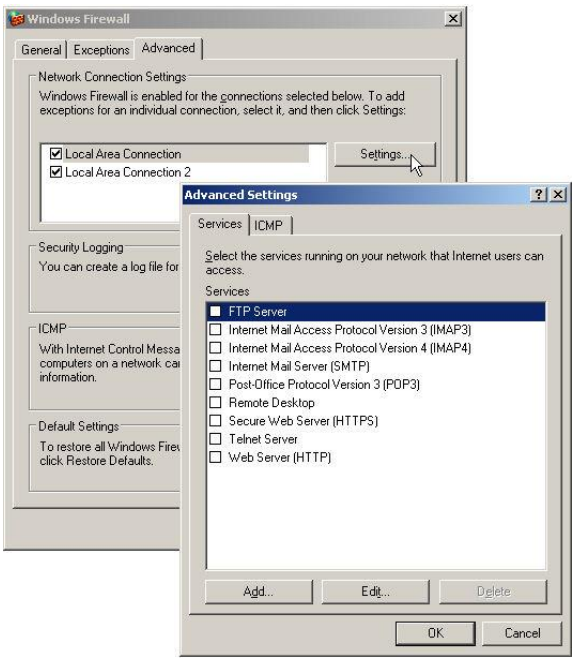


Connection Specific Configuration Options

On computers with multiple connections, Windows Firewall also allows per-connection configuration. All connection-specific configurations will override global configuration. Connection specific configurations can be set by selecting a connection from the **Network Connections Settings**, of the **Advanced** tab in the **Windows Firewall** interface, and editing its settings.

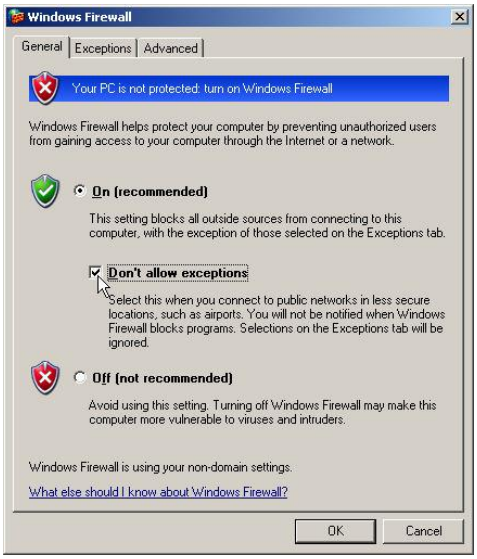
Copyright © 2008 Microsoft Corporation.

All rights reserved.



Operating Modes for Excepted Traffic

Windows Server 2003 with SP2, provides a new operating mode corresponding to the **Don't allow exceptions** check box on the **General** tab of the **Windows Firewall** interface. When Windows Firewall is running in this new mode, all unsolicited incoming traffic is dropped, including excepted traffic. This new mode can be used when connecting the computer to an untrusted network environment, or to lock down computers temporarily during a network attack or when a malicious program is spreading. Once the network attack is over and appropriate updates are installed to prevent future attacks, the Windows Firewall can be placed in the normal operating mode that allows authorized excepted traffic. All of the original settings for excepted traffic are maintained.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

Startup Security

Prior to Windows Server 2003 SP1, the windows firewall (formerly known as the Internet Connection Firewall (ICF)) was activated only after the ICF/Internet Connection Sharing (ICS) service started successfully after system startup. Therefore, on Windows Server 2003 computers not using SP1 or higher, there is a delay between when the computer is active on the network and when the connections are protected with the built-in firewall. This delay makes the computer vulnerable to attacks during the startup process.

In Windows Server 2003 with SP1 and higher, there is a static rule called a **boot-time policy** to perform stateful packet filtering, which allows the computer to perform basic networking startup tasks using DHCP and the DNS protocol to configure the computer and communicate with a Domain Controller to obtain Group Policy updates. Once the Windows Firewall/ICS service is started, it uses its configuration and removes the **boot-time policy**. There is no boot-time security if the **Windows Firewall/ICS** service is set to **Disabled**. The **boot-time policy** configuration settings cannot be modified.

Incoming Traffic Scoping for IPv4

Prior to Windows Server 2003 SP1, the excepted traffic could originate from any IPv4 address. In Windows Server 2003 with SP1 and higher, the Windows Firewall allows authorized administrators to specify that excepted traffic can originate from any IPv4 address, from an IPv4 address that matches the local subnet to which the connection that received the traffic is attached, from one or more specific IPv4 addresses, or from one or more ranges of IPv4 addresses. This is known as configuring the incoming traffic scope.

Built-in Support for IPv6

The Windows Firewall includes IPv6 support and automatically enables IPv6 on all connections. Both IPv4 and IPv6 share the same settings for excepted traffic. For example, if an authorized administrator excepts file and print sharing traffic, then both IPv4 and IPv6-based unsolicited incoming file and print sharing traffic is allowed.

For incoming IPv6 traffic, Windows Firewall allows authorized administrators to specify that excepted traffic can originate from any IPv6 address or from an IPv6 address that matches the local subnet to which the connection that received the traffic is attached.

Note: Windows Firewall does not support the same scope options for IPv6 traffic as IPv4 traffic.

Specifying Exempted Traffic by Program File Name

Prior to Windows Server 2003 SP1, excepted traffic was configured by specifying the set of TCP and UDP ports that correspond to the traffic of a specific program, which can be either an application or service. This can make configuration difficult if the set of TCP and UDP ports for the application or service or how to find them is not known. Also, this configuration does not work for applications that do not listen on a specific set of UDP or TCP ports.

To make the specification of excepted traffic easier, it is possible in Windows Server 2003 with SP1 and higher to configure excepted traffic by either specifying the set of TCP or UDP ports or the filename of the program (application or service). When the program runs, Windows Firewall monitors the ports on which the program listens and automatically adds them to the list of excepted traffic.

To allow authorized administrators to quickly enable exceptions for commonly allowed incoming unsolicited traffic, Windows Firewall has pre-defined exceptions, such as File and Printer Sharing and Remote Assistance. Additionally, the notification mechanism in Windows Firewall allows authorized

Copyright © 2008 Microsoft Corporation.

All rights reserved.

administrators to automatically add new programs to the excepted programs list after being prompted with a Windows Security Alert message.

Windows Firewall Group Policy Settings

To centralize the configuration of large numbers of computers in an organization network that use Active Directory, Windows Firewall settings for computers running Windows Server 2003 with SP2 can be deployed through Computer Configuration Group Policy. A new set of Computer Configuration Group Policy Windows Firewall settings allow a network administrator to configure Windows Firewall operational modes, excepted traffic, and other settings using a GPO.

When the Windows Firewall configured in an organization network using Group Policy, some of the local Windows Firewall configuration options can be grayed out and unavailable, even for local administrators. For details on configuring the Windows Firewall through a domain level Group Policy, see Configuring Windows Firewall through domain Group Policy settings.

Windows Firewall and the Impact to Enterprise Networks

For enterprise networks, enabling Windows Firewall on all network connections on servers may have a significant impact on the types of communication that can occur. If the Windows Server 2003 computers are only running client-based programs, then the Windows Firewall will not impair communications. Web access, email, Group Policy, and management agents that request updates from a management server are examples of client-based programs. For client-based programs, the client computer always initiates the communication and all response traffic from a server is allowed by Windows Firewall because it is solicited incoming traffic.

However, the consequences to blocking all unsolicited incoming traffic by default can affect network services if the computers running Windows Server 2003 are managed, and are providing network services that require clients to initiate contact with the server such as file services, application hosting, print services, etc. To prevent this from happening, a Windows Server 2003 server that has the Windows Firewall enabled must be configured with the appropriate Windows Firewall exception settings to allow the computer to act as a managed computer and provide access to the services it is providing for the network.

Using the Windows Firewall and IPSec

Windows Firewall blocks unsolicited incoming traffic. However, administrators cannot configure Windows Firewall to block outgoing traffic. IPSec, built into Windows Server 2003, can be configured to provide this extra level of protection. Using IPSec policies, authorized administrators can specify the traffic that is blocked (dropped), permitted (allowed), or protected using cryptography for both outgoing and incoming traffic. In any of these three cases (blocked, permitted, protected), IPSec can be configured for a specific range of source and destination addresses. For details on configuring IPSec policies on Windows Server 2003, see the Configuring IPSec Policies subsection of this document.

If IPSec is already being used to block, permit, or protect traffic, then Windows Firewall on computers running Windows Server 2003 can be used to provide additional protection from attacks based on incoming unsolicited traffic.

IPSec in Windows Server 2003 with SP2 is Windows Firewall-aware. When there is an active IPSec policy, the IPSec components of Windows Server 2003 instruct the Windows Firewall to open UDP ports 500 and 4500 to allow IKE traffic.

An additional feature of IPSec support is that authorized domain administrators can specify through Group Policy that all IPSec-protected traffic bypass Windows Firewall processing. For details on setting a Group Policy for IPSec, see the Configuring IPSec Policies subsection of this document.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

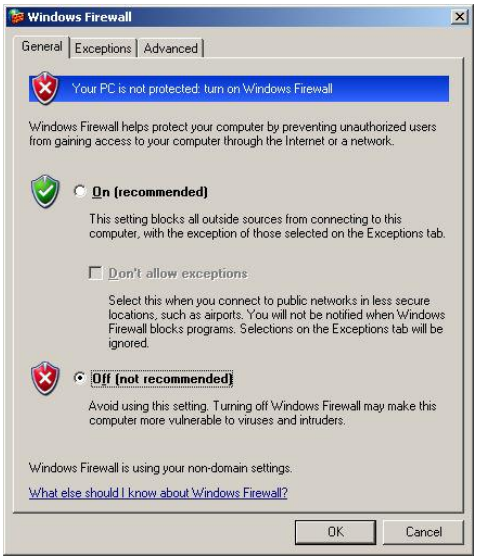
Configuring Windows Firewall Settings

This subsection defines the various setting options available in through Windows Firewall interface and provides procedures for configuring those options.

Note: If a domain Group Policy is used to configure Windows Firewall for domain members, the Group Policy settings may not allow local configuration. In this case, the configuration options described below may be grayed out and unavailable, even to members of the local Administrators group.

To enable the Windows Firewall and modify settings:

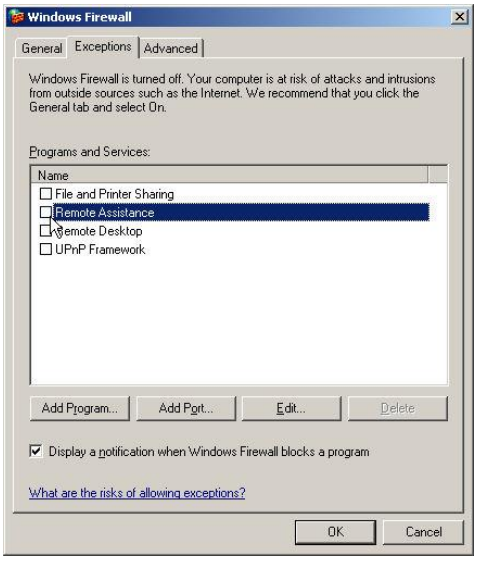
1. Log on as an authorized administrator.
2. Click **Start**, point to **Control Panel**, and select **Windows Firewall**.



3. The **General** tab of the **Windows Firewall** interface provides the following operating mode options:
   - **On (recommended).** This option enables Windows Firewall for all of the network connections that are explicitly selected on the **Advanced** tab. By default, Windows Firewall is enabled to allow only solicited and excepted incoming traffic. Excepted traffic must be explicitly configured on the **Exceptions** tab.
   - **Don't allow exceptions.** Select this check box to allow only solicited incoming traffic. Any excepted incoming traffic defined on the **Exceptions** tab will not be allowed.
   - **Off (not recommended).** This is the default setting on Windows Server 2003. Select this option to disable Windows Firewall.
4. Select the **On (recommended)** radio button to enable the firewall.
5. To add or modify firewall exceptions, select the **Exceptions** tab. Uncheck the **Remote Assistance** check box. **Remote Assistance** is not used in the Evaluated Configuration.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

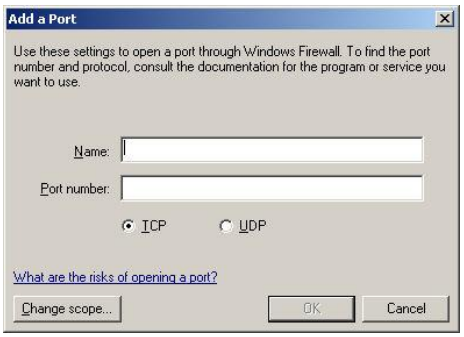


- To allow an exception for a program or service currently listed in the list of **Programs and Services**, check the box next to the desired program or service name.
- To add a new service or program to the list of **Programs and Services**, click the **Add Programs** button. The **Add a Program** interface will appear. Click the **Browse** button to find and add a specific application not listed in the default list of programs. Select the program from the list and click **OK**. The program will appear selected in the list of **Programs and Services**.

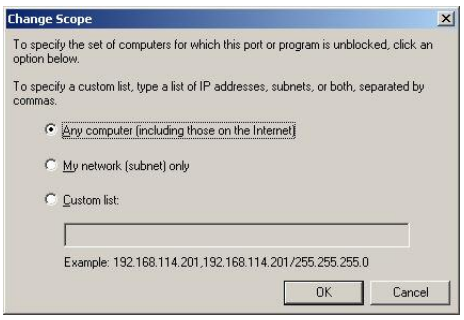
- To create an exception for a specific TCP or UDP port, click the **Add a Port** button on the **Exceptions** tab of the **Windows Firewall** interface. Specify a port name that will be displayed in the list of **Programs and Services**, enter the port number, and select the TCP or UDP radio button, as appropriate. Click **OK**. The port will appear selected in the list of **Programs and Services**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



- Windows Firewall allows authorized administrators to specify the scope of excepted traffic. The scope defines the portion of the network from which the excepted traffic is allowed to originate. To define the scope for a program or port, click **Change Scope**. The **Change Scope** button is available on both, the **Add a Program** and the **Add a Port** interfaces.



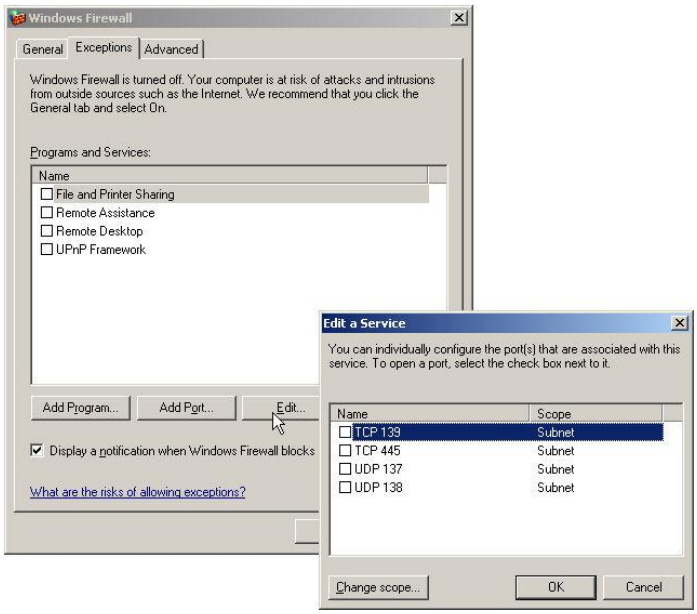
The **Change Scope** interface provides three scope options:

- **Any computer (including those on the Internet).** Excepted traffic is allowed from any IPv4 address. This setting may make the computer vulnerable to attacks from malicious users or programs on the Internet.
- **My network (subnet) only.** Excepted traffic is allowed only from an IPv4 address that matches the local network segment (subnet) to which the network connection that received the traffic is attached.
- **Custom list.** This scope option allows an authorized administrator to specify one or more IPv4 addresses or IPv4 address ranges separated by commas. IPv4 address ranges typically correspond to subnets. For IPv4 addresses, type the IPv4 address in dotted decimal notation. For IPv4 address ranges, specify the range using a dotted decimal subnet mask or a prefix length. When using a dotted decimal subnet mask, specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When using a network prefix length, specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). An example custom list is the following: 10.91.12.56,10.7.14.9/255.255.255.0,10.116.45.0/255.255.255.0,172.16.31.11/24,172.16.111.0/24.

Note: It is not possible to specify a custom list for IPv6 traffic.

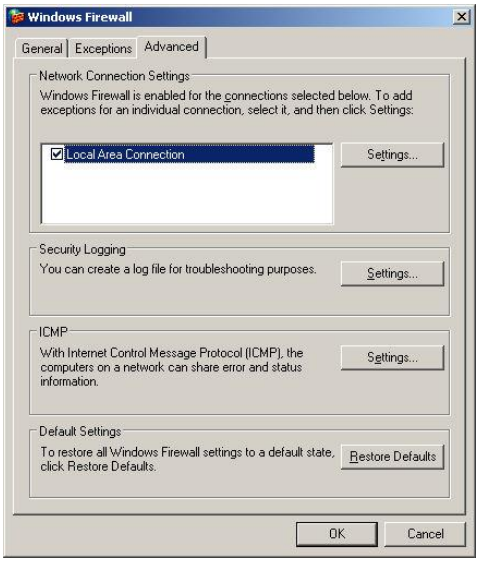
- To modify an existing exception, select the exception from the list of **Programs and Services** on the **Exceptions** tab of the **Windows Firewall** interface and click the **Edit** button. Make the necessary changes in the **Edit a Service** interface. The configuration options available in the **Edit a Service** interface will vary depending on the specific programs or service.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



- To remove an excepted program or service from the available list, select the program or service and click the delete button. Programs and services that are listed by default in the Windows Firewall **Exceptions** tab cannot be deleted.

6. To modify settings individually for network connections, create a log file, configure ICMP settings, or restore **Windows Firewall** settings to their default configuration, select the **Advanced** tab of the **Windows Firewall** interface.

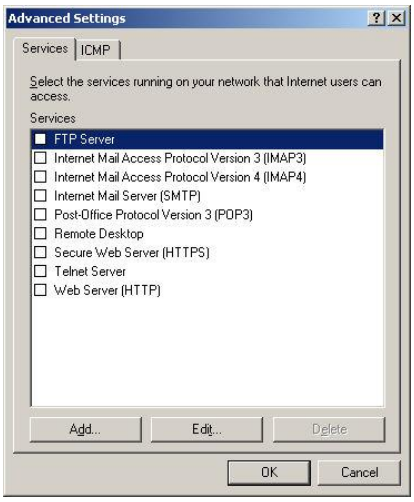


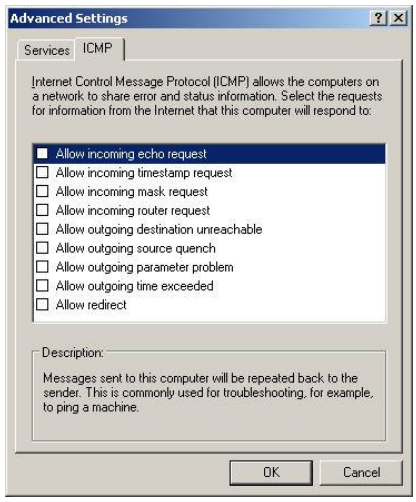
- If there are more than one network interfaces and they require unique configuration settings, select the network connection from the list displayed in the **Network Connection Settings** selection box and click the **Settings** button. The **Advanced Settings** interface for the selected network connection will appear. The **Advanced Settings** interface allows authorized administrators to configure specific services from the **Services** tab (by TCP or UDP port only) or enable specific types of ICMP traffic from the **ICMP** tab.

Warning: If the checkbox for any of the network connections listed in the **Network Connection Settings** selection box is cleared, that connection will not be protected by the Windows Firewall.

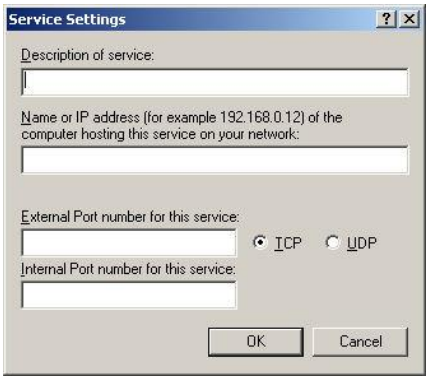
Copyright © 2008 Microsoft Corporation.

All rights reserved.

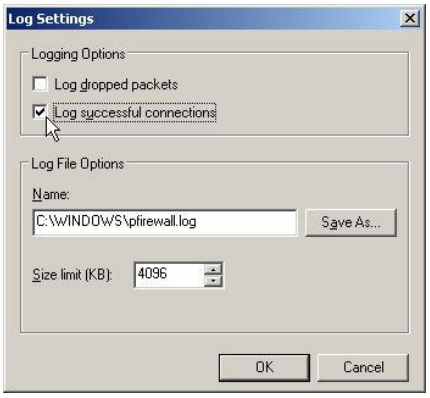




- To add a service, click the **Add** button on the **Services** tab of the **Advanced Settings** interface. In the **Service Settings** interface, enter a description of the service, its address information, and the port information as required. Click **OK** to add the service to the **Services** list.

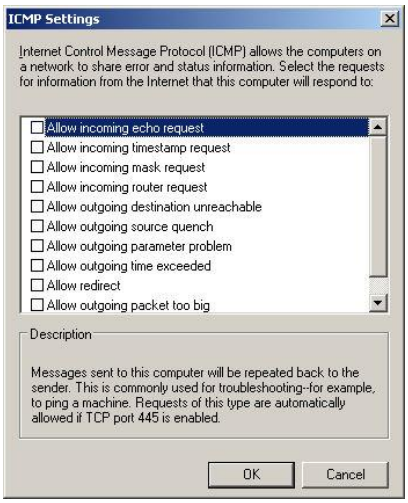


- Select the **Edit** button to edit the settings for a selected service. Except for specifying a network address, services listed by default cannot be edited.
- To modify ICMP settings, select the ICMP tab and select or deselect from the list of ICMP services. ICMP services cannot be added or modified.
- To modify Windows Firewall log settings, select the **Settings** button in the **Security Logging** section of the Windows Firewall **Advanced** tab. Use the **Log Settings** interface to select logging options for dropped packets and successful connections, change the location of the log file, or change the log size.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

- To modify global ICMP settings for all network connections, click the **Settings** button in the **ICMP** section of the Windows Firewall **Advanced** tab. Select or deselect from the list of ICMP services. ICMP services cannot be added or modified.



- To restore all Windows Firewall settings to their default configuration, click the **Restore Defaults** button in the **Default Settings** section of the Windows Firewall **Advanced** tab. A confirmation window will appear, click **Yes** to restore the default settings.

Configuring Windows Firewall through Domain Group Policy Settings

The best way to manage Windows Firewall settings in an organization network is to use Active Directory and the new Windows Firewall settings in the Computer Configuration component of Group Policy. This method requires the use of Active Directory with Windows Server 2003 Domain Controllers. Group Policy updates are requested by the domain member computer, and are therefore solicited traffic that is not dropped when Windows Firewall is enabled on a client. Starting with Windows Server 2003 SP1 introduced a new set of Computer Configuration Group Policy Windows Firewall settings was introduce that allow authorized network administrator to configure Windows Firewall operational modes, excepted traffic, and other settings using a GPO.

When a Group Policy is used to configure Windows Firewall, by default local administrators will be unable to change some elements of its configuration locally, using the Windows Firewall component in Control Panel. Some tabs and options in the Windows Firewall dialog box will be grayed out and unavailable to local administer accounts.

The following subsections describe these steps for using the Computer Configuration component of Group Policy to configure Windows Firewall across a domain, site, or OU.

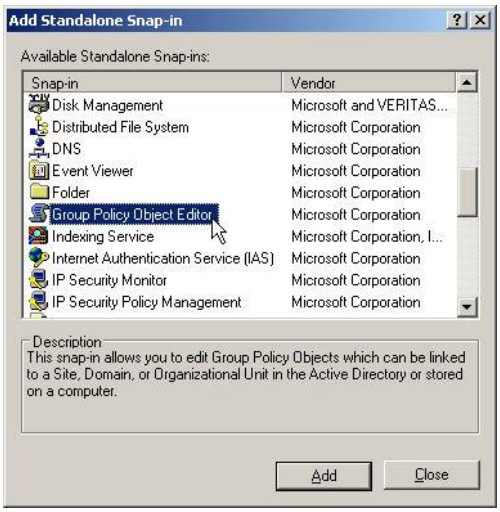
Note: It is strongly recommended that Windows Firewall Group Policy settings be tested in a lab environment prior to deploying them in to a production environment in order to ensure that the Windows Firewall Group Policy configuration does not result in unintended problems affecting business operations.

Copyright © 2008 Microsoft Corporation.

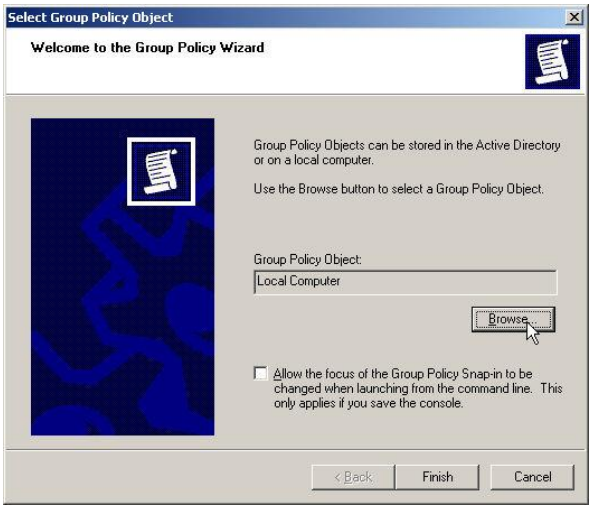
All rights reserved.

Accessing the Windows Firewall Settings in the Domain Local Policy GPO

1. Log on to the Domain Controller as an authorized administrator.
2. Click **Start**, click **Run**, type **mmc** in the **Open** box, and click **OK**.
3. On the **Console** menu, click **Add/Remove snap-ins**, and click **Add**.
4. Locate the **Group Policy Object Editor** snap-in, and click **Add**.

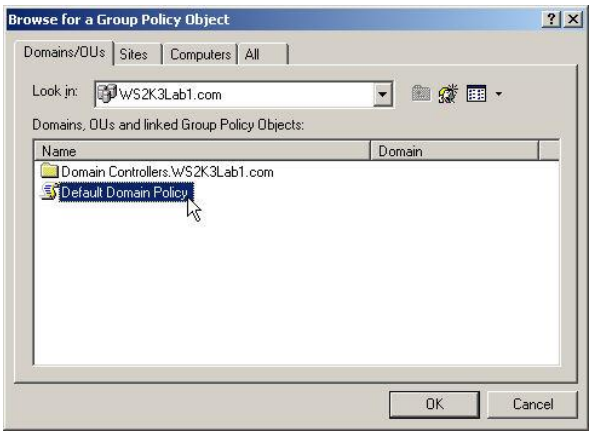


5. In the **Select Group Policy Object** wizard, click **Browse**. Click **Close**. Click **OK**.

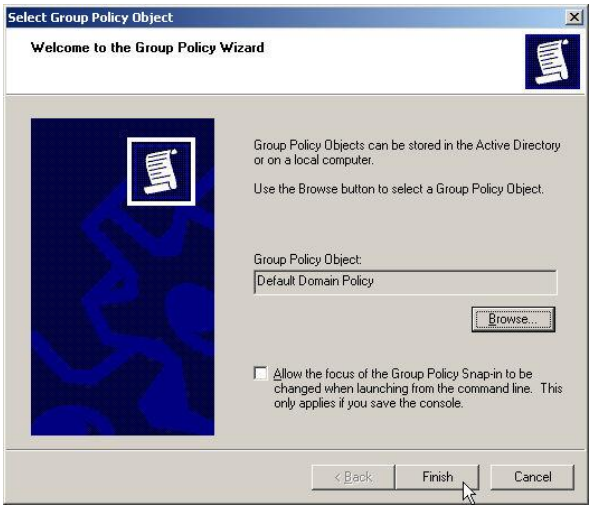


6. In the **Browse for a Group Policy Object** interface, select find and select the desired GPO. For this example, select the **Default Domain Policy**. Click **OK**.

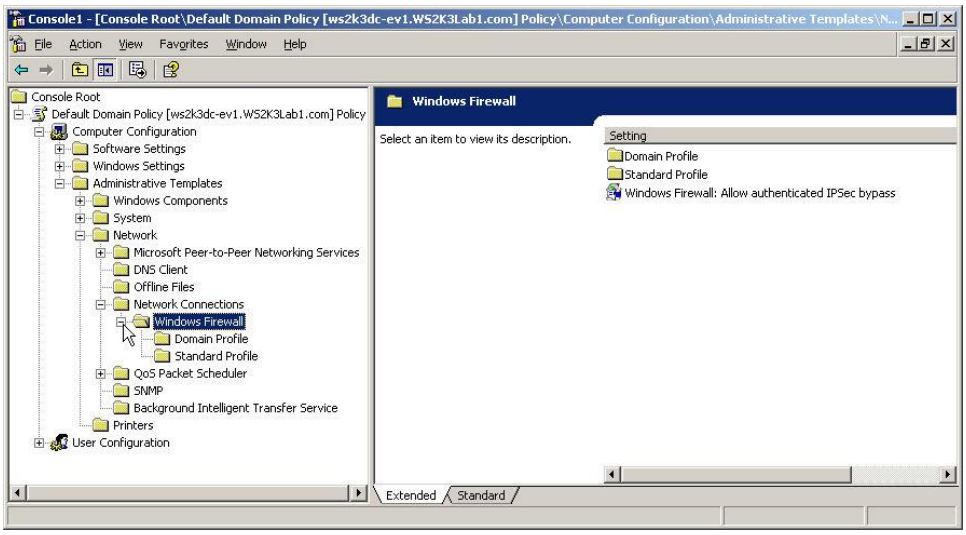
Copyright © 2008 Microsoft Corporation.
All rights reserved.



7. Click **Finish** to complete the **Select Group Policy Object** wizard. Click **Close**. Click **OK**.



8. In the console tree, expand the GPO object (**Default Domain Policy**), **Computer Configuration**, **Administrative Templates**, **Network**, **Network Connections**, and then **Windows Firewall**.



9. Two different Windows Firewall profiles are visible. Windows Server 2003 and Windows XP Professional with SP2 rely on network determination to determine which profile settings to apply. For more information, see Network Determination Behavior for Network-Related Group Policy Settings.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Domain Profile**. The **Domain Profile** is the set of Windows Firewall settings that are needed when the computer is connected to a network that contains the Domain Controllers of the organization. For example, the domain profile might contain excepted traffic for the applications needed by a managed computer in an enterprise network.
- **Standard Profile**. The **Standard Profile** is the set of Windows Firewall settings that are needed when the computer is not connected to a network that contains the Domain Controllers of the organization. A good example is when an organization laptop is taken on the road and connects to the Internet using a public broadband or wireless Internet service provider. Because the organization laptop is directly connected to the Internet, the standard profile should contain more restrictive settings than the domain profile.

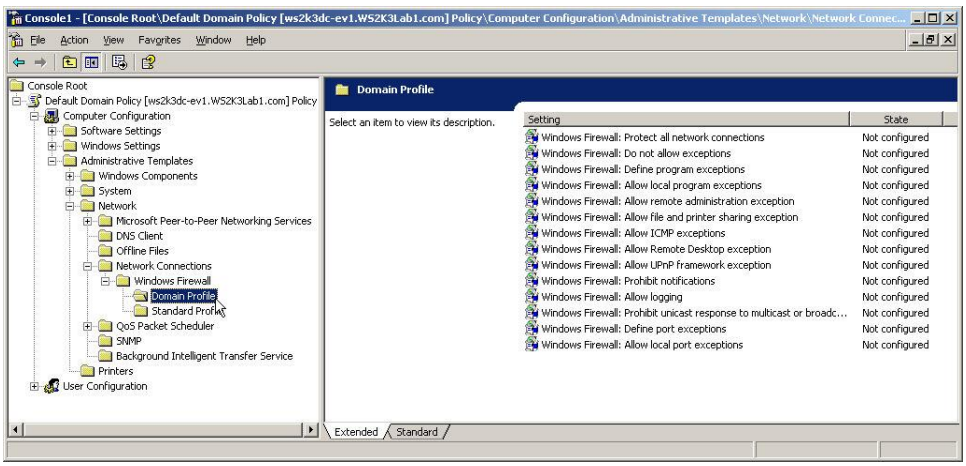
Note: Enabling Windows Firewall for both profiles is strongly recommended.

Specifying Windows Firewall Settings in a Group Policy

If the **Standard Profile** settings are not configured, their default values are still applied. Therefore, it is highly recommended that both the **Domain Profile** and **Standard Profile** settings are configured and that the Windows Firewall is enabled for both profiles.

As previously described, the **Standard Profile** settings are typically more restrictive than the **Domain Profile** settings because the **Standard Profile** settings do not need to include applications and services that are only used in a managed domain environment.

Both the **Domain Profile** and **Standard Profile** contain the same set of Windows Firewall settings.



The Windows Firewall Group Policy settings for the domain and standard profiles consist of the following:

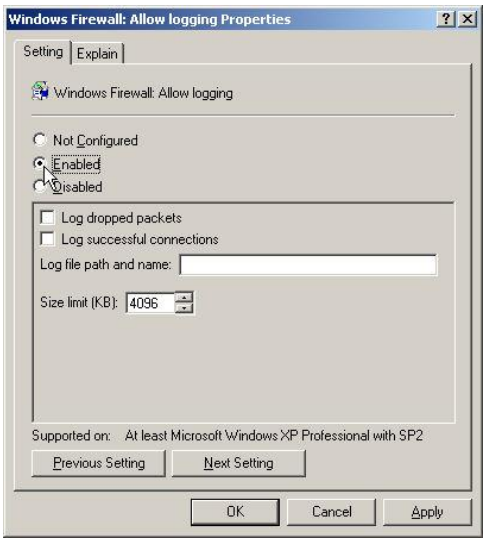
- **Windows Firewall: Protect all network connections.** Used to specify that all network connections have Windows Firewall enabled.
- **Windows Firewall: Do not allow exceptions.** Used to specify that all unsolicited incoming traffic be dropped, including excepted traffic.
- **Windows Firewall: Define program exceptions.** Used to define excepted traffic in terms of program file names.
- **Windows Firewall: Allow local program exceptions.** Used to enable local configuration of program exceptions.
- **Windows Firewall: Allow remote administration exception.** Used to enable remote configuration using tools such as MMC and WMI.

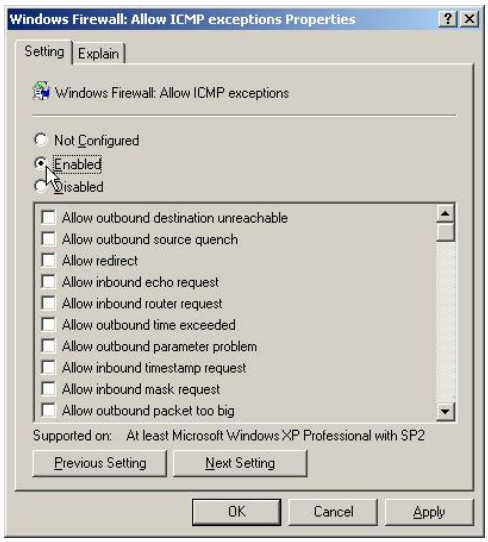
Copyright © 2008 Microsoft Corporation.
All rights reserved.

- **Windows Firewall: Allow file and print sharing exception.** Used to specify whether file and printer sharing traffic is allowed.
- **Windows Firewall: Allow ICMP exceptions.** Used to specify the types of ICMP messages that are allowed.
- **Windows Firewall: Allow Remote Desktop exception.** Used to specify whether the Windows XP-based computer can accept a Remote Desktop-based connection request.
- **Windows Firewall: Allow UPnP framework exception.** Used to specify whether the computer can receive unsolicited UPnP messages.
- **Windows Firewall: Prohibit notifications.** Used to disable notifications.
- **Windows Firewall: Allow logging.** Used to enable logging of discarded traffic, successful connections, and to configure log file settings.
- **Windows Firewall: Prohibit unicast response to multicast or broadcast requests.** Used to discard the unicast packets received in response to a multicast or broadcast request message.
- **Windows Firewall: Define port exceptions.** Used to specify excepted traffic in terms of TCP and UDP ports.
- **Windows Firewall: Allow local port exceptions.** Used to enable local configuration of port exceptions.

To modify a Windows Firewall Group Policy settings:

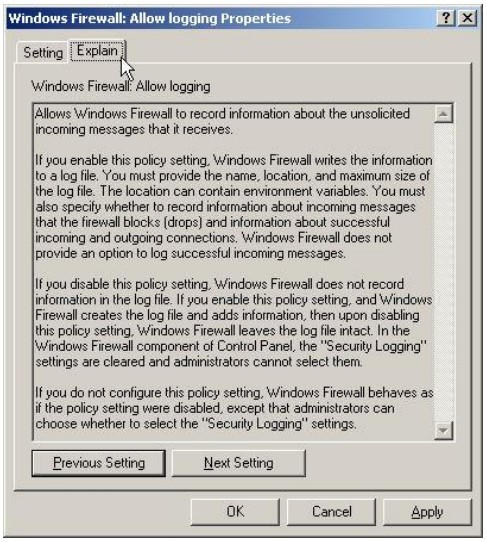
1. Double-click on the setting or right-click it and select **Properties**.
2. The **Properties** interface for the Windows Firewall Group Policy setting will appear.
3. On the **Setting** tab view, select to enable, disable, or not configure the setting. There are additional setting options available that will vary according to the setting objectives.





4. The **Explain** tab views for each setting provide a detailed explanation of the setting functions.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



Once the Windows Firewall settings are configured, the next refresh of Computer Configuration Group Policy downloads the new Windows Firewall settings and applies them for computers running Windows XP Professional with SP2 and Windows Server 2003 with SP2. Any computers that are running Windows 2000, Windows Server 2003, Windows XP with SP1, or Windows XP with no service packs installed will ignore the new Windows Firewall settings.

Automated Configuration of Windows Firewall with SCW

Security Configuration Wizard (SCW) is a new feature in Windows Server 2003 with SO1 that provides guided attack surface reduction for Windows Server 2003 servers. The SCW is highly recommended for automating the configuration of Windows Firewall on and creating security lockdown templates for servers based on their roles. When the SCW is used to secure a server based on its defined functional roles, the Windows Firewall is automatically enabled and configured by SCW to block all ports that are not needed by the defined server roles. See Security Configuration Wizard for details about SCW.

See the Securing an IIS 6.0 host with the Security Configuration Wizard subsection for a detailed example of how to use the **Security Configuration Wizard**.

SCW

SCW is a new feature in Windows Server 2003 with SP1 and higher that provides guided attack surface reduction for Windows Server 2003 servers. SCW is highly recommended for automating the configuration of Windows Firewall on and creating security lockdown templates for servers based on their roles.

When using the SCW to lockdown a server, authorized administrators will be asked a series of questions to determine the functional requirements of their server based on the specific roles of the server will be performing. Any functionality that is not required by the roles the server is performing will be disabled or blocked from use.

SCW uses a roles-based metaphor driven by an extensible Extensible Markup Language (XML) knowledge base that defines the services, ports, and other functional requirements for over 50 different server roles including roles for Windows Server System applications such as Microsoft Exchange Server and Structured Query Language (SQL) Server.

SCW uses this extensible XML knowledge base to perform role discovery, solicit user input, and author security policies that disable services, block ports, modify registry values, and configure audit settings. Even ports that are left open can be restricted to specific populations or secured using IPSec. SCW also

Copyright © 2008 Microsoft Corporation.

All rights reserved.

allows authorized administrators to roll back previously applied policy settings. SCW also integrates with Active Directory to support deployment of SCW-generated policy settings through Group Policy.

The SCW allows authorized administrators to easily:

- Disable unnecessary services.
- Disable unnecessary IIS Web extensions.
- Block unused ports, including support for multi-homed scenarios.
- Secure ports that are left open using IPSec.
- Reduce protocol exposure for Lightweight Directory Access Protocol (LDAP), LAN Manager, and SMB.
- Configure audit settings with a high signal-to-noise ratio.
- Import Windows security templates for coverage of settings that are not configured by the wizard.

In addition to roles-based, guided security policy authoring, SCW also supports:

- **Rollback**. Enables authorized administrators to return their servers to the state it was in before they applied the SCW security policy, which can be useful when applied policies disrupt service expectations.
- **Analysis**. Enables authorized administrators to check that servers are in compliance with expected policies.
- **Remote access**. Supports remote access for configuration and analysis operations.
- **Command line support**. A command-line tool is provided for remote configuration and analysis of groups of servers.

  Note: The SCW command-line tool is not a component of the Windows Server 2003 Evaluated Configuration.

- **Active Directory integration**. Supports deploying SCW policies using Group Policy.
- **Editing**. A security policy created using SCW can be modified when necessary, such as when machines are repurposed.
- **XSL views**. Provides the ability to view the data stored in the knowledge base, policies, and analysis results XML files.

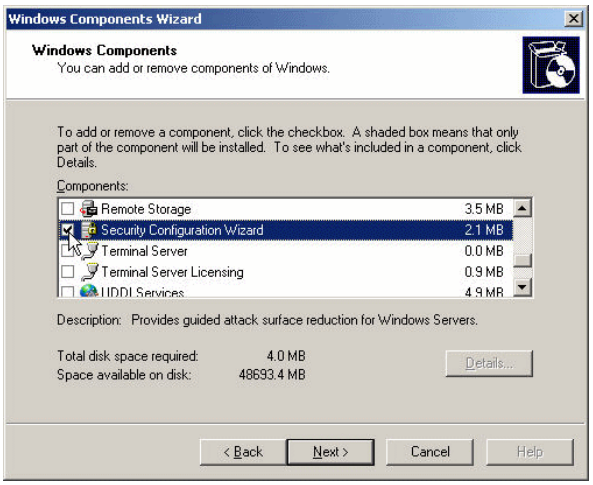
Installing the Security Configuration Wizard

The SCW is included with the installation of Windows Server 2003 SP2, but is not installed by default. To install the SCW:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
3. On the **Add or Remove Programs** interface, click the **Add/Remove Windows Components** button to start the **Windows Components Wizard**.
4. In the **Windows Components** list, scroll down and select the **Security Configuration Wizard** by clicking the check box next to it. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. The **Windows Component Wizard** begins the installation of components. When it is completed, click the **Finish** button.

6. Close the **Add or Remove Programs** interface.

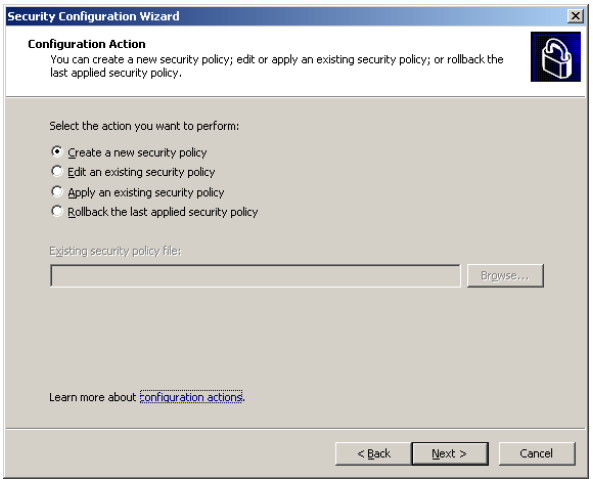
Accessing the Security Configuration Wizard

Once installed thorough the **Windows Components Wizard**, the SCW will be accessible from the **Administrative Tools** menu.

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Security Configuration Wizard**. The **Security Configuration Wizard** interface will be displayed.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. To use the Wizard, click Next. A list of action options will appear as shown below.



- **Create a new security policy**. This option allows authorized administrators to create a security policy that configures services, Windows Firewall, IPSec settings, audit policy, and specific registry settings. The security policy is an XML file that can be edited and applied with SCW. The policy can later be made into a GPO by using the scwcmd.exe command-line tool. For more information about Scwcmd.exe, see Security Configuration Wizard command-line tool.

- **Edit an existing security policy**. This option allows authorized administrators to edit a security policy that was previously created with SCW. **Edit an existing security policy** must be selected in order to browse to the location of the security policy that is to be edited. The policy that is edited can be stored locally or in a network shared folder. SCW can edit policies with an .xml file name extension. Authorized administrators must use the SCW to edit any security policy previously created with SCW. Manually editing the XML security policy is not supported. Security templates with an .inf extension cannot be edited with SCW.

- **Apply an existing security policy**. Once a security policy is created with SCW, it can be applied it to a test server for testing purposes or to a production environment. The Scwcmd.exe command-line tool can be used to apply the same policy to multiple servers. Authorized administrators can use the **scwcmd transform** command to create GPOs. The SCW can apply XML security policies, but does not recognize any other file types.

  If the selected server is a member of an Active Directory domain, then domain-based GPO security policy generally overrides registry settings set directly through SCW. If this is not desired, create a GPO by using **scwcmd transform** and apply it through Active Directory.

Copyright © 2008 Microsoft Corporation.

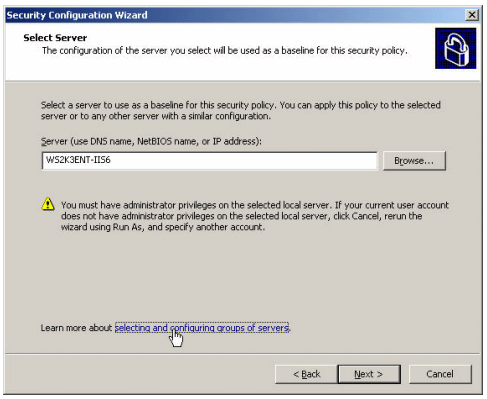
All rights reserved.

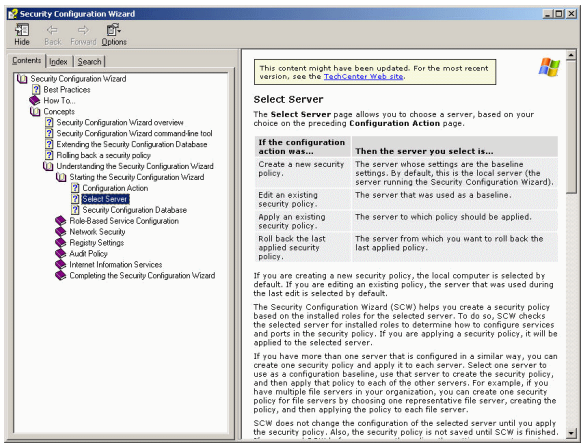
Note: It is highly recommended that a newly-created or modified security policy be tested before applying it to a production environment. Testing minimizes the possibility that the new policy might cause unexpected behavior, such as compatibility issues, in a production environment.

- **Rollback the last applied security policy**. If a security policy applied with SCW causes decreased functionality for a server or other undesirable results, it can be rolled back so that it is no longer applied to the server. However, if the policy is edited in Local Security Policy after it is applied, the changes are not be rolled back to their pre-application state. They remain in their current configuration.

  For services and registry values, the process of rolling back restores settings that were changed during the configuration process. For Windows Firewall and IPSec, the process of rolling back unassigns any SCW policy that is currently in place and reassigns the previous policy that was in place at configuration time.

4. Select the desired action and click **Next** to follow instructions from the Wizard. Each Wizard view has a "**Learn more about**…" link that opens a help file with details about the current window options. Use the help files for assistance in making the proper selections.





See the Securing an IIS 6.0 host with the Security Configuration Wizard subsection for a detailed example of how to use the **Security Configuration Wizard**.

SCW Command-line Tool

Installed with the SCW is the **Scwcmd.exe command-line tool**. **Scwcmd.exe** can be used for the following tasks:

- Configure one or many servers with an SCW-generated policy.
- Analyze one or many servers with an SCW-generated policy.
- View XML policy files or analysis results in HyperText Markup Language (HTML).
- Roll back SCW policies.
- Transform an SCW-generated policy into native files that are supported by Group Policy.
- Register a knowledge base extension with SCW.

To get basic help on the **Scwcmd.exe command-line tool**, at a command prompt, type ***scwcmd*** and press the **Enter** key on the keyboard. The following information will be presented.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

```
Command line supplement for the SCW.

Syntax: scwcmd [analyze | configure | register | rollback | transform | view ]
```

For further help, type ***scwcmd*** along with any of the options above to present more details for that option. For example, typing ***scwcmd analyze*** will present the following information.

```
Determines whether a machine is in compliance with a policy. Results are returned in an XML
accepts a list of machines as input. To view the analysis results in your browser, use `scw
and specify %windir%\security\msscw\transformfiles\scwanalysis.xsl as the XSL transform.

Syntax: scwcmd analyze [[[/m:machine | /ou:ou] /p:policy] | /i:machinelist] [/o:resultdir]
[/u:username] [/t:threads] [/l] [/e]

/m:machine     Specifies the NetBIOS Name, DNS Name or IP Address of the machine to analyze
specified,              then /p must also be specified.

/ou:ou         Specifies the Fully Qualified Domain Name (FQDN) of an OU in the Active Dire
If /ou is specified, then /p must also be specified. All machines in the OU will be analyze
the given policy.

/p:policy              Specifies the path and filename of the xml policy file that should be
perform the analysis.

/i:machinelist Specifies the path and filename of an xml file that contains a list of machi
with their                    expected policy files. All machines in the xml file will be a
against their corresponding policy                  files. See
%windir%\security\msscw\kbs\SampleMachineList.xml

/o:resultdir   Specifies the path and directory where the analysis result files should be d
Default is the                        current directory.

/u:username    Specifies an alternate credential to use when performing the analysis on a r
machine. Default                      is the logged on username.

/t:threads             Specifies the number of simultaneous outstanding analysis operations
be maintained                 during the analysis process. Default is 40.

/l             Causes the analysis operation to be logged. One log file will be generated f
machine being                 analyzed.  The log files will be stored in the same directory
result files.  Use the /o option to                 specify the directory for the result fi

/e             Log an event to the Application Event Log if a mismatch is found.

Examples:

scwcmd analyze /p:webpolicy.xml

scwcmd analyze /m:webserver /p:webpolicy.xml /u:webadmin

scwcmd analyze /i:campusmachines.xml /t:100 /o:\\resultserver\results

scwcmd analyze /ou:OU=WebServers,DC=Marketing,DC=ABCCompany,DC=com /p:webpolicy.xml /u:Doma
```

IIS 6.0

To help protect systems from attackers who target unused or unmonitored services, IIS 6.0 is not installed on Windows Server 2003 by default. An authorized administrator must install IIS 6.0 manually when it is needed. In addition, when IIS is initially installed, the service is installed in a secure, "locked" mode.

In Windows Server 2003, IIS can be installed by using either the **Windows Component Wizard** from the **Control Panel** or the **Configure Your Server Wizard** from the **Manage Your Server** interface. These options offer slightly different default installations:

- By using the **Add or Remove Programs** in **Control Panel**, a **Windows Component Wizard** guides the installation. By default, the **Windows Component Wizard** only enables and installs IIS, therefore the default installation will only serve static content. Features such as Active Server Pages (ASP), ASP.NET, Server-Side Includes (SSI), WebDAV publishing, Microsoft Distributed Transaction

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Coordinator (DTC), and FrontPage Server Extensions are either not installed or not enabled, and therefore do not work by default. However, they are options that may be selected during the Wizard installation process.

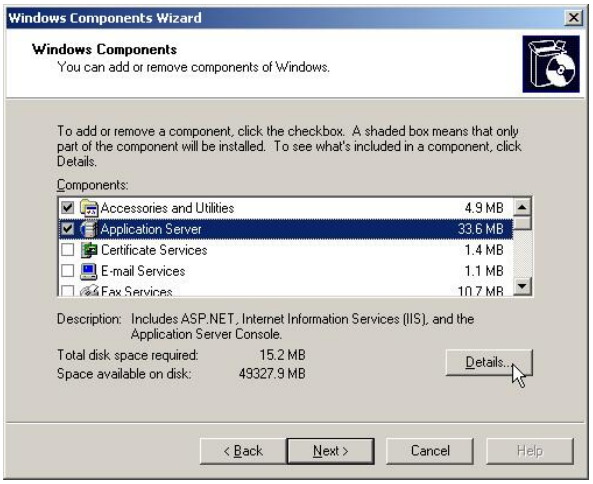
- By using the **Configure Your Server Wizard**, ASP.NET and ASP are automatically installed with IIS. In addition, there are options for enabling ASP.NET and installing FrontPage Server Extensions by using the wizard.

Note: For the Evaluated Configuration, it is best to follow the procedures below to install IIS using the **Windows Component Wizard,** which does not, by default, install components that are not included in the Evaluated Configuration.

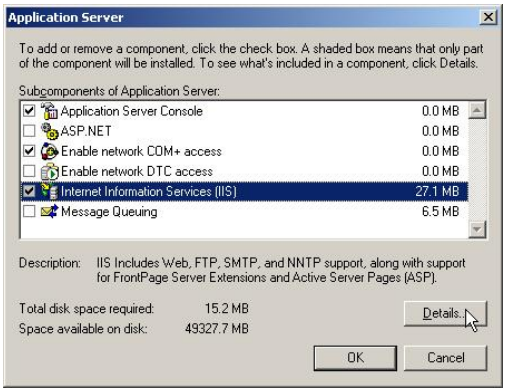
Installing IIS 6.0

The following steps show how to install IIS.

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
3. On the **Add or Remove Programs** interface, click the **Add/Remove Windows Components** button to start the **Windows Components Wizard**.
4. In the **Windows Components** list, select the check box next to **Application Server**, and click the **Details** button.



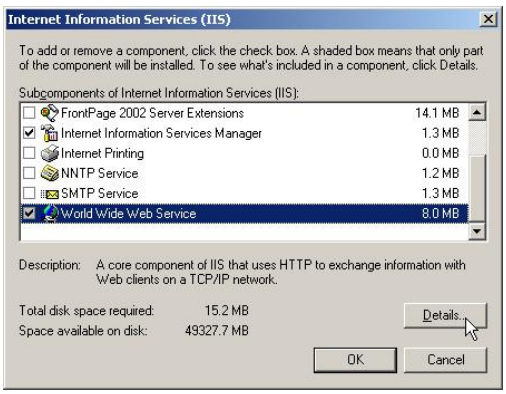
5. In the **Application Server** interface, notice what is installed by default. Under **Subcomponents of Application Server**, select **Internet Information Services (IIS)** and click **Details**.



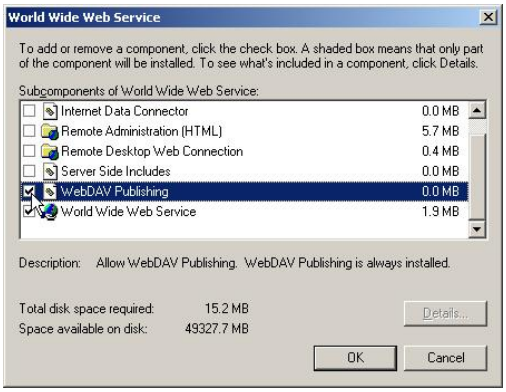
Copyright © 2008 Microsoft Corporation.

All rights reserved.

6. In the **Internet Information Services (IIS)** interface, notice what is installed by default. In the **Subcomponents of Internet Information Services (IIS)** list, select **World Wide Web Service** and click **Details**. For the Evaluated Configuration, **Internet Printing** may also be selected if needed.



7. In the **World Wide Web Service** interface, notice what is installed by default. To add optional subcomponent, select the check box next to the subcomponent that that is to be added. To remove optional subcomponent, clear the check box next to the subcomponent that is to be removed. In the example below, **WebDAV Publishing** is selected as an added subcomponent.

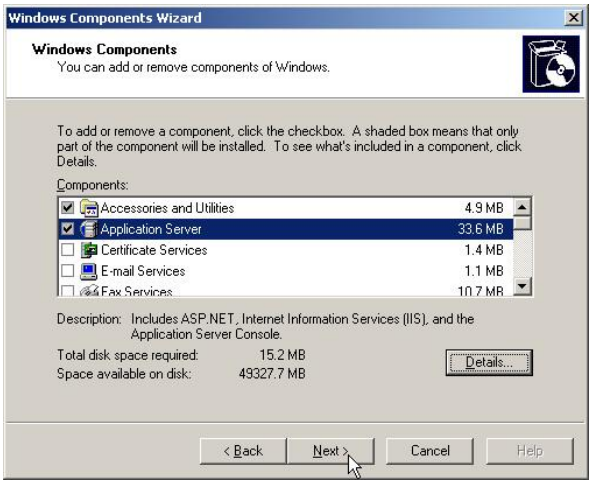


8. For the Evaluated Configuration, the ASPs subcomponent must be unselected by clearing its check box. A message will appear indicating that Internet Printing is dependent on ASP. Removing ASP will disable the ability to connect to printers via a Web page, however users can still connect to the printers by using the printer's URL. See "Connect to a Printer Using a URL" for the procedures. Click **Yes** on the **Setup** message and then click **OK** on the **World Wide Web Service** interface.

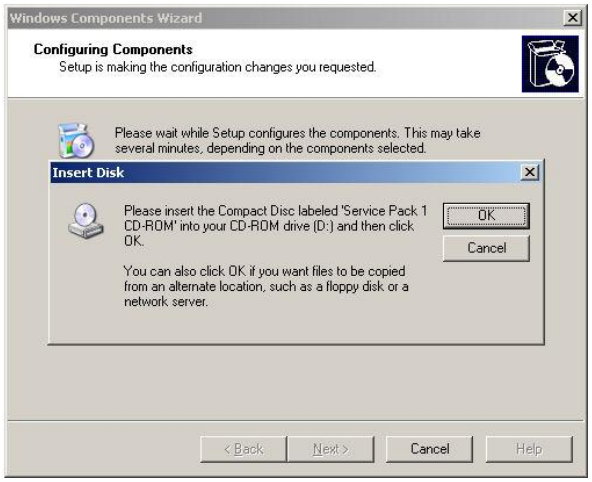
9. Click **OK** on the **Internet Information Services (IIS)** interface, click **OK** on the **Application Server** interface, then click **Next** on the **Windows Component Wizard**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



10. If the Windows Server 2003 installation disk is not in the CD-ROM drive, a message will appear asking that it be inserted. Insert the installation disk for Windows Server 2003 in the CD-ROM drive to allow the IIS installation to continue.



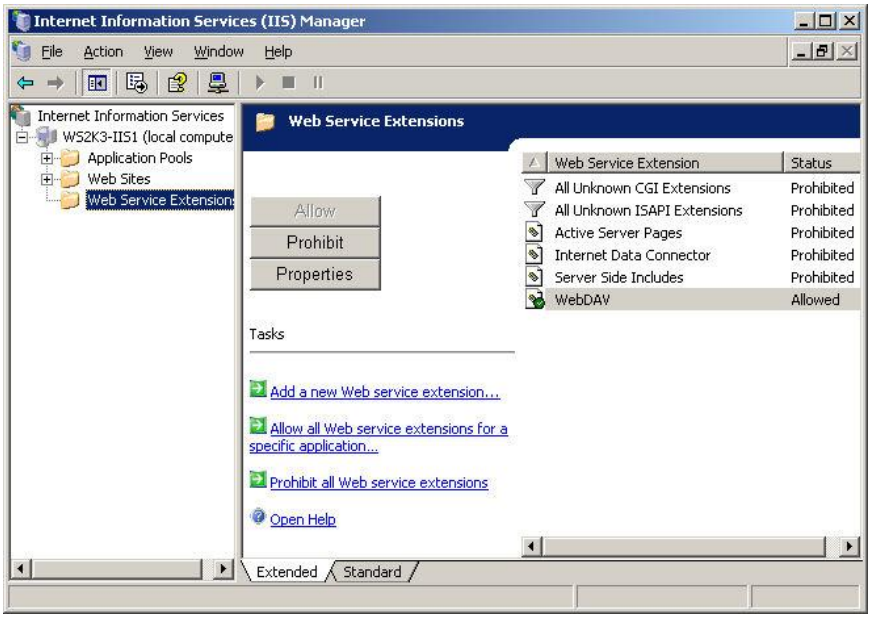
11. When the installation process is complete, click **Finish** on the **Windows Component Wizard**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

IIS Manager

To access the IIS management interface:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.



IIS Web Site Authentication

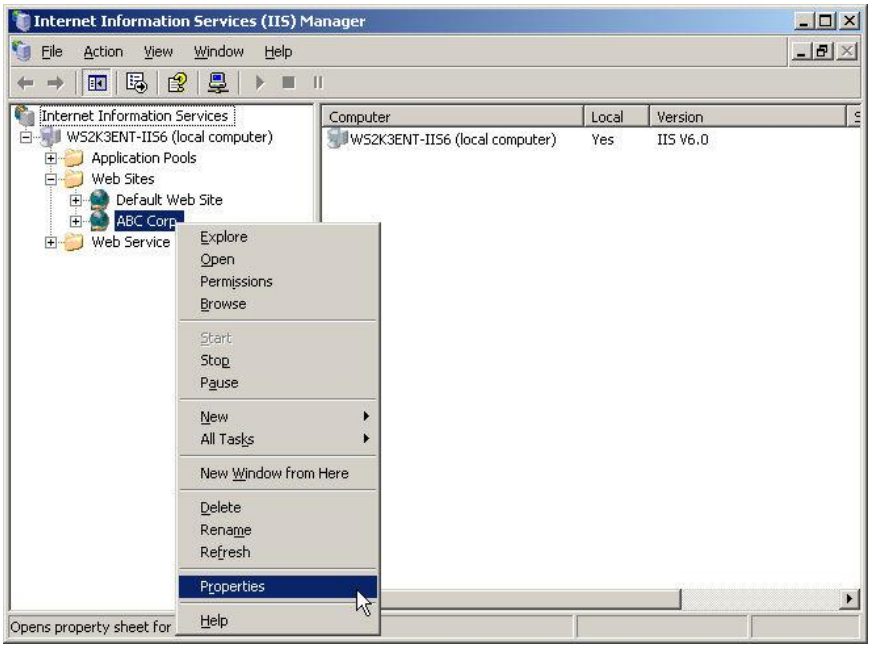
Authorized administrators can configure IIS to authenticate users before they are permitted access to a Web site, a folder in the site, or even a particular document contained in a folder in the site. Authentication in IIS can be used to strengthen the level of security on sites, folders, and documents that are not to be viewed by the general public.

Authentication Based on User Credentials

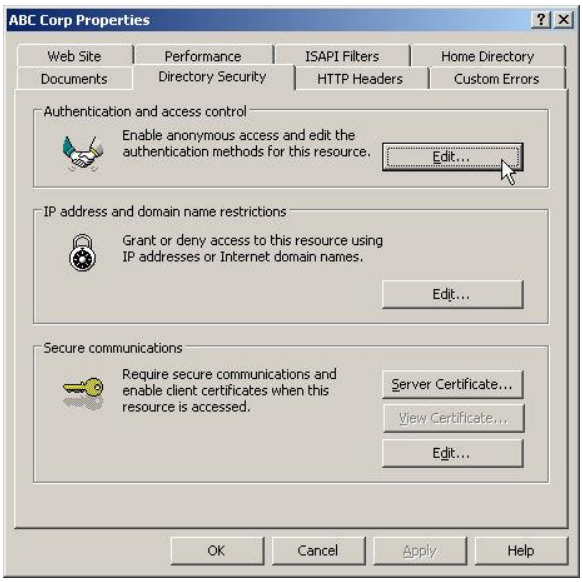
To configure authentication in IIS based on user credentials:

1. Log on as an authorized administrator.
2. Open the **Internet Information Services (IIS) Manager** interface.
3. Expand ***Server_name***, where *Server_name* is the name of the server, and then expand **Web Sites**.
4. In the console tree, right-click the Web site, virtual directory, or file for which authentication is to be configured, and then click **Properties**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. Click the **Directory Security** or **File Security** tab and then under **Anonymous and access control**, click **Edit**.



6. Click to select the check box next to the authentication method or methods to be used, and then click **OK**. The authentication methods that are set by default are **Anonymous access** and **Integrated Windows authentication**. The following authentication options are available on the **Authentication Methods** interface:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: If multiple authentication options under **Authenticated access** are selected, IIS tries to negotiate the most secure method first, and then it works down the list of available authentication protocols until a mutual authentication protocol is supported by both client and server.

- **Anonymous access**: When anonymous access is turned on, no authenticated user credentials are required to access the site. This option is best used to grant public access to information that requires no security. When a user tries to connect to the Web site, IIS assigns the connection to the ***IUSER_ComputerName*** account, where *ComputerName* is the name of the server on which IIS is running. By default, the ***IUSER_ComputerName*** account is a member of the Guests group. This group has security restrictions, imposed by NTFS file system permissions that designate the level of access and the type of content that is available to public users.

Warning: If anonymous access is turned on, IIS always tries to authenticate users by using anonymous authentication first, even if additional authentication methods are turned on. Therefore, to use an authentication method selected under **Authenticated access**, the **Enable anonymous access** check box must not be checked.

- **Integrated Windows Authentication**: Formerly named *NTLM* or *Windows NT Challenge/Response authentication*, this method sends user authentication information over the network as a Kerberos ticket, and provides a high level of security. Windows Integrated authentication uses Kerberos version 5 and NTLM authentication. To use this method, clients must use Microsoft Internet Explorer 2.0 or later. Additionally, Windows Integrated authentication is not supported over HTTP proxy connections.

Note: For Windows Integrated Authentication to work with an IIS Web site (that is not installed on a Domain Controller), the IIS computer must be trusted for delegation in Active Directory in order for Kerberos to function properly. See the Trust for Delegation Configuration in Active Directory for IIS Hosts subsection for details.

- **Digest authentication for Windows domain servers**: Digest authentication requires a user ID and password, provides a medium level of security, and may be used to grant access to secure information from public networks. This method offers the same functionality as basic authentication. However, this method transmits user credentials across the network as an MD5 hash, or *message digest*, in which the original user name and password cannot be deciphered from the hash. To use this method, clients must use Microsoft Internet Explorer (IE) 5.0 or later, and the Web clients and Web servers must be members of, or be trusted by, the same domain.

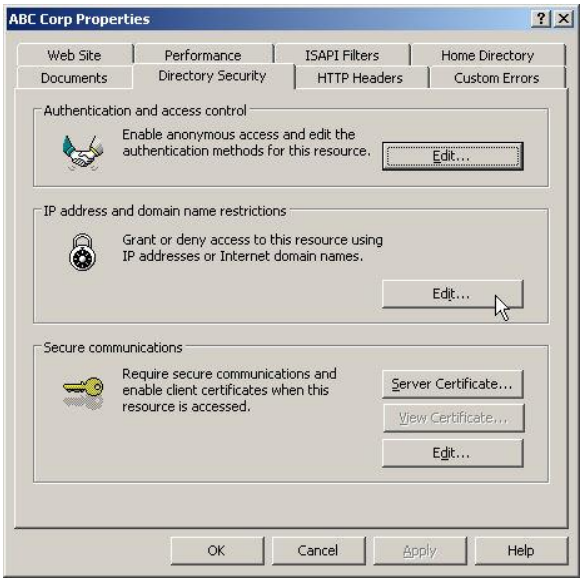
Copyright © 2008 Microsoft Corporation.
All rights reserved.

- **Basic authentication (password is sent in clear text)**: Basic authentication requires a user ID and password, and provides a low level of security. User credentials are sent in clear text across the network. This format provides a low level of security because the password can be read by almost all protocol analyzers. ***This option must not be used for the Evaluated Configuration***.
- **Microsoft .NET Passport authentication**: .NET Passport authentication provides single sign-in security, which provides users with access to diverse services on the Internet. When this option is selected, requests to IIS must contain valid .NET Passport credentials on either the query string or in the cookie. If IIS does not detect .NET Passport credentials, requests are redirected to the .NET Passport logon page. ***This option must not be used for the Evaluated Configuration***.

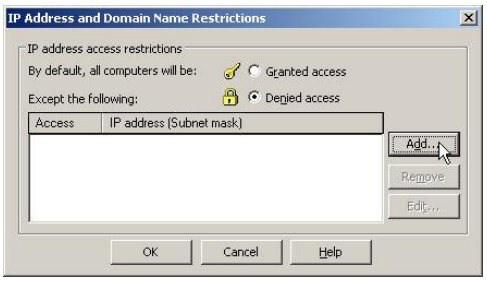
Authentication Based on Requesting Host

Another type of authentication is based on the requesting host instead of on user credentials. Authorized administrators can limit access based on source IP address, source network ID, or source domain name.

1. To grant or deny access to specific computers, groups of computers, or domains, click **Edit** under **IP Address and Domain Name Restrictions in the Directory Security tab of the Printers Properties interface**.



2. In the **IP Address and Domain Name Restrictions** dialog box that is displayed, complete one of the following procedures:
   - To explicitly grant access:
     - Select the **Denied Access** radio button to deny access to all computers by default, and then click the **Add button to create exceptions for computers that will be explicitly granted access**.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

- In the **Grant Access On** dialog box, select the desired option and then click **OK**. The computer, group of computers, or domain selected is added to the **Granted** list.

- To explicitly deny access:
  - Select the **Granted Access** radio button to grant access to all computers by default, and then click **Add button to create exceptions for computers that will be explicitly denied access**.
  - In the **Deny Access On** dialog box that is displayed, specify the desired option and then click **OK**. The computer, group of computers, or domain specified is added to the **Denied** list.
- Click **OK**.

3. Click **OK**, and then quit **IIS Manager.**

Notes:

A prompt may appear to apply any changes that have made to existing sites. If the authentication changes need to be applied to other content, click the content from the list of child nodes, and then click **OK**. If the changes are not to be applied to any of the child nodes, do not select any items on the list, and then click **OK**.

In IIS, authentication options can be set at the Web site, directory, or file level. The same principles that are discussed in this article apply to each.

Trust for Delegation Configuration in Active Directory for IIS Hosts

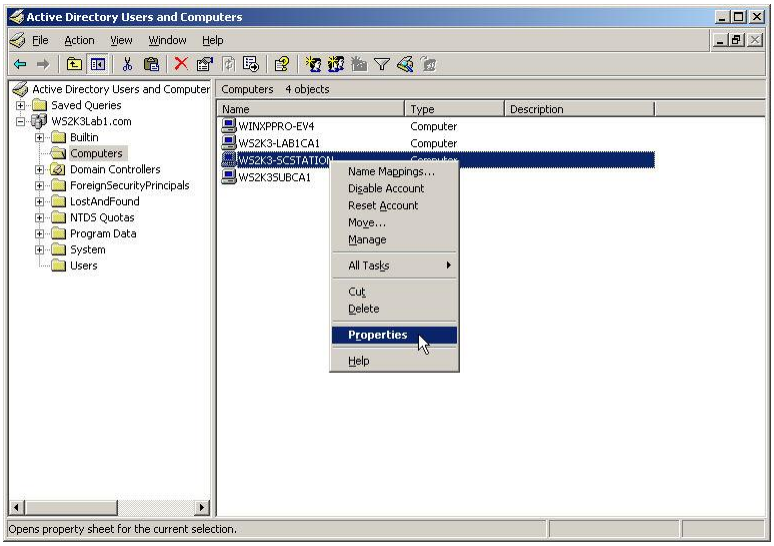
To use Window Integrated Authentication for an IIS Web site not configured on a Domain Controller, the IIS host must be trusted for delegation in order to forward authentication requests. To configure a computer to be trusted for delegation:

Note: The procedures below apply to Domain Controllers that have been set to a **Windows Server 2003 Domain Functional Level**.

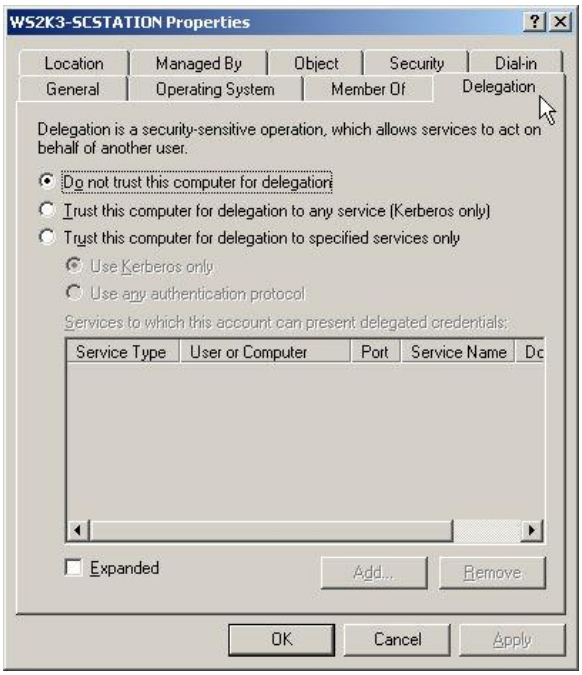
---

1. Log onto the Domain Controller with Domain Administrator rights.
2. Click **Start**, point to **Administrative Tools**, and select **Active Directory Users and Computers**.
3. Expand the domain node and select the **Computers** folder.
4. Right-click the computer that is hosting IIS and select **Properties**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



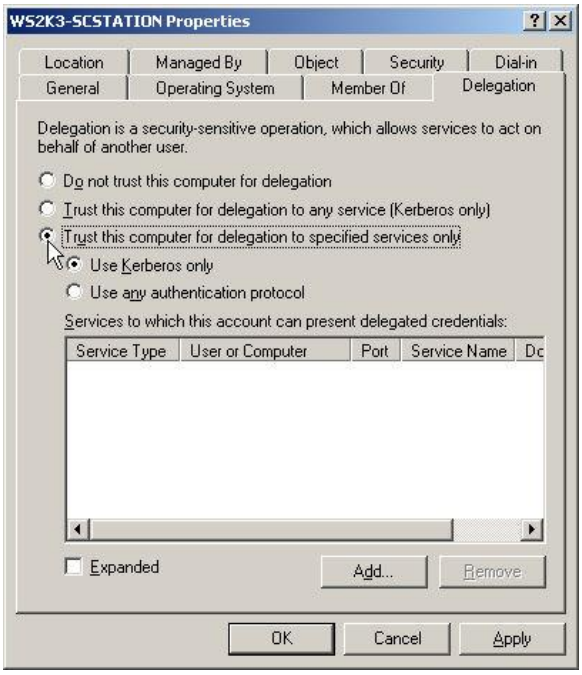
5. In the computer **Properties** interface, select the **Delegation** tab.



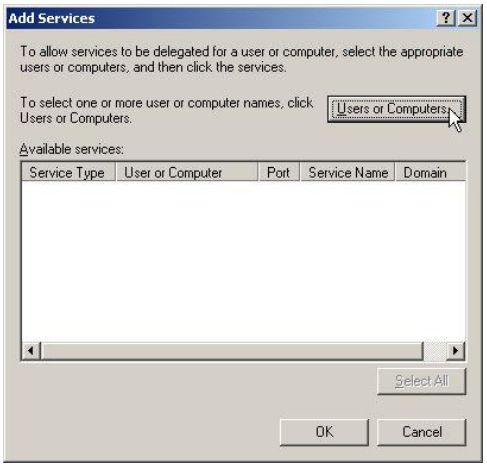
6. Select the **Trust this computer for delegation to specified services only** radio button and the **Use Kerberos only** radio button. Click Add.

Copyright © 2008 Microsoft Corporation.

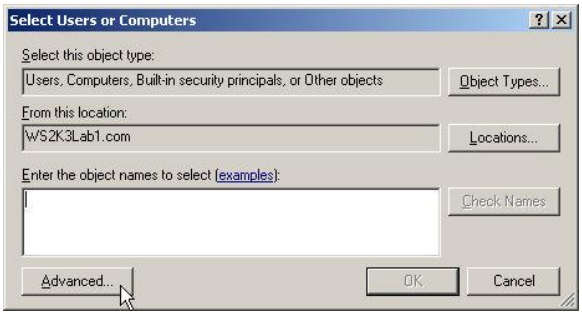
All rights reserved.



7. Click the **Users or Computers** button on the **Add Services** interface.

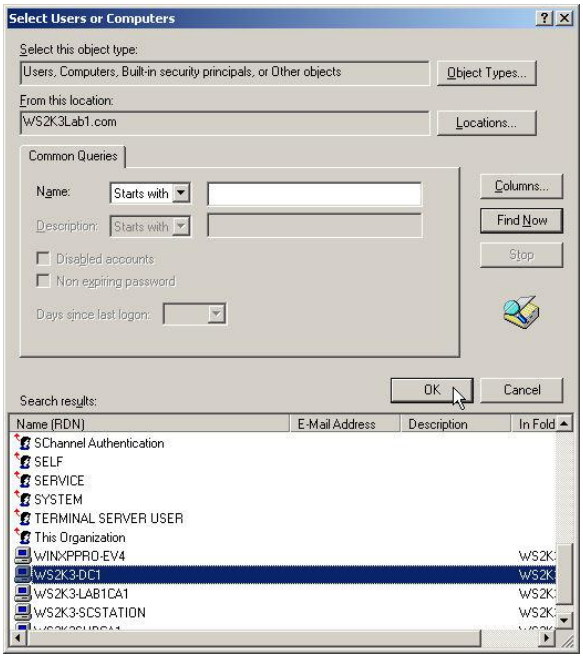


8. Click the **Advanced** button on the **Select Users or Computers** interface.

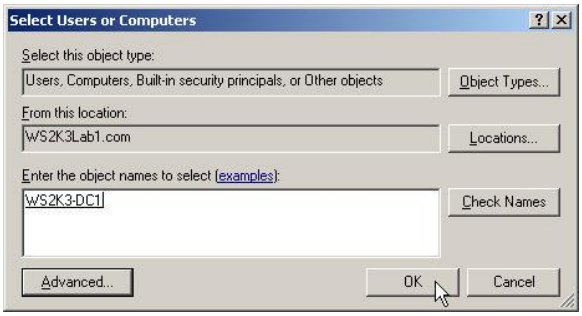


9. Click the **Find Now** button on the next **Select Users or Computers** interface, then select the computer that is to receive the user's credentials from IIS (in this example, we will be passing the credentials directly to the Domain Controller). Click **OK**.

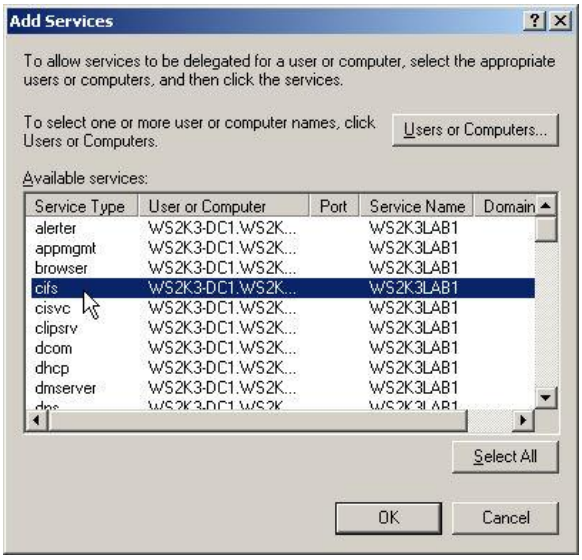
Copyright © 2008 Microsoft Corporation.
All rights reserved.



10. Click OK on the **Select Users or Computers** interface.



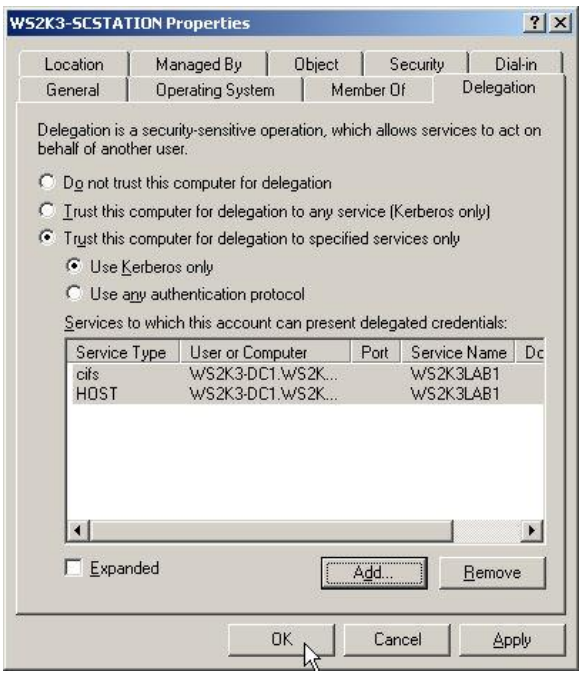
11. The **Add Services** dialog box now shows the services that are registered as Service Principal Names (SPNs) with Kerberos for the selected computer. Hold down the **<Ctrl>** key on the keyboard and select the **HOST** (the server service) and Common Internet File System (**CIFS**) from the **Service Type** list. Click **OK**.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

12. From the **Delegation** tab on the computer **Properties** interface, verify that the new services were added in the **Services to which this account can present delegated credentials** dialog box. Click **OK** to close the computer **Properties** interface.



IIS Virtual Directories

A virtual directory is a friendly name, or alias, either for a physical directory on a server hard drive that does not reside in the home directory, or for the home directory on another computer. Because an alias is usually shorter than the path of the physical directory, it is more convenient for users to type. The use of aliases is also secure because users do not know where files are physically located on the server and therefore cannot use that information to modify the files. Aliases also make it easier to move directories in a site. Rather than changing the URL for the directory, authorized administrators can change the mapping between the alias and the physical location of the directory.

If a Web site contains files that are located in a directory other than the home directory, or on other computers, authorized administrators must create virtual directories to include those files in their Web site. To use a directory on another computer, authorized administrators must specify the directory's Universal Naming Convention (UNC) name, and provide a user name and password for access rights.

To publish from any directory not contained within a home directory, authorized administrators must create a virtual directory. For example, for a Web site set up for a marketing team, the following table shows the mapping between the physical location of the files and the URL that accesses the files.

Physical Location	Alias	URL
C:\Inetpub\wwwroot	home directory (none)	http://SampleWebSite
\\Server2\SalesData	Customers	http://SampleWebSite/Customers
D:\Inetpub\wwwroot\Quotes	None	http://SampleWebSite/Quotes
D:\Inetpub\wwwroot\OrderStatus	None	http://SampleWebSite/OrderStatus
D:\Marketing\PublicRel	PR	http://SampleWebSite/PR

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Both virtual directories and physical directories (directories without an alias) appear in IIS Manager. A virtual directory is indicated by a gear icon.

For a simple Web site, there may be no need to add virtual directories. All of the files can simply be placed in the site's home directory. If there is a complex site, or to specify different URLs for different parts of a site, add virtual directories as needed. To make a virtual directory accessible from multiple sites, add the virtual directory to each site.

To create a virtual directory using the Virtual Directory Creation Wizard:

1. In IIS Manager, double-click the local computer, double-click the Web site to which a virtual directory is to be added, right-click the Web Site or folder within which to create the virtual directory, point to **New**, and then click **Virtual Directory**.
2. Click **Next**.
3. In the **Alias** box, type a name for the virtual directory, and then click **Next**. The alias is the name that the user types, and it should be short and easy to type.
4. In the **Directory** box, type or browse to the physical directory in which the virtual directory resides, and then click **Next**.
5. In the **Access Permissions** dialog box, set the appropriate access permissions based on operational needs.
6. Click **Next**, and then click **Finish**.

To create a virtual directory by importing a configuration file:

1. In IIS Manager, double-click the Web site to which a virtual directory is to be added, right-click the Web Site or folder where the virtual directory is to be created, point to **New**, then click **Virtual Directory (from file)**.
2. Click **Next**.
3. In the **Import configuration** box, click **Browse** and navigate to the file containing the virtual directory configuration to import.
4. Click **Read File**, click the virtual directory configuration to import, and then click **OK**.

To create a virtual directory using Windows Explorer:

1. In Windows Explorer, browse to the folder where a virtual directory is to be created, right-click the directory, and click **Sharing and Security**.
2. Click the **Web Sharing** tab, and in the **Share on** list box, click the site for which a virtual directory is being created, and click **Share this folder**.
3. In the **Alias** box, type an alias name for this virtual directory.
4. Set the **Access permissions** and **Applications permissions** by clicking the appropriate settings.
5. Click **OK**, and then click **OK** again. Verify that the virtual directory was created by starting IIS Manager and double-clicking the Web site.

To delete a virtual directory using IIS Manager:

In IIS Manager, expand the site containing the virtual directory to be deleted, right-click the virtual directory, click **Delete**, and then click **Yes**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

To delete a virtual directory using Windows Explorer

1. In Windows Explorer, browse to the folder containing the virtual directory to be deleted, right-click the directory, and click **Sharing and Security**.
2. Click the **Web Sharing** tab, click **Remove**, and then click **Yes**.
3. Click **OK**. Verify that the virtual directory was deleted by starting IIS Manager and double-clicking the Web site.

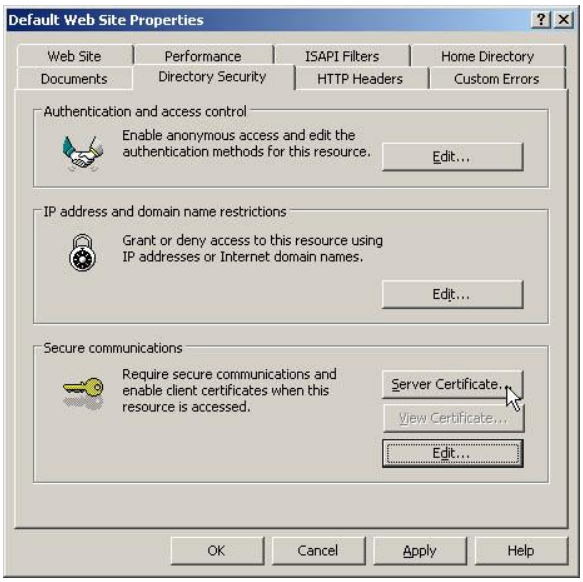
Configuring SSL on a Web Server or Web Site

To enable SSL on a Web site, a server certificate must first be requested from a trusted CA. After obtaining the certificate, it must be installed on the Web server, and then assigned to one or more Web sites.

Request a Server Certificate

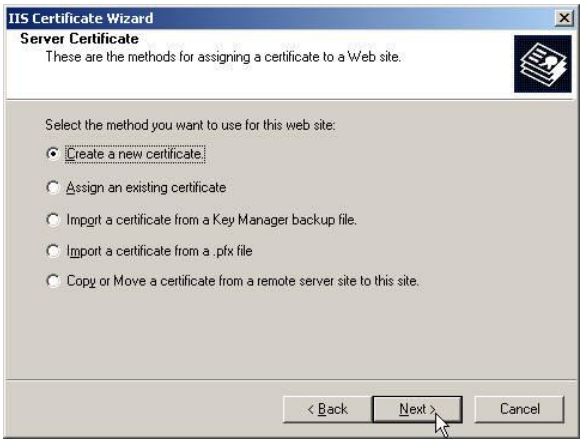
To request a server certificate:

1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. Expand ***Server_name***, where *Server_name* is the name of the server, and then expand **Web Sites**.
4. In the console tree, right-click the Web site or file which is to be protected with SSL, and then select **Properties**.
5. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.

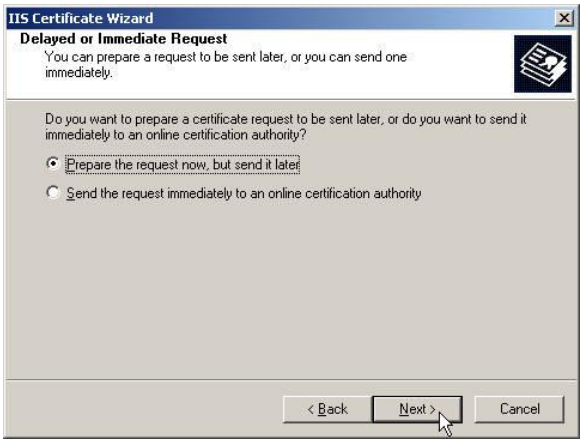


6. In the **Web Server Certificate Wizard**, click **Next**.
7. Select the **Create a new certificate** radio button and click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



8. On the **Delayed or Immediate Request** view of the Wizard, select whether to prepare a request or to send the request immediately to an online CA. If an online CA is not available, or accessible by the Web server host, the **Send the request to an online certification authority** radio button will be grayed out.



9. To prepare a request file, select the **Prepare the request now, but send it later** radio button and click **Next**. Continue at Step 11.
10. To send a request immediately to an online CA, select the **Send the request to an online certification authority** radio button and click **Next**. If there is a pending request, a notice will appear stating that it will be deleted, click **Next**.
11. In the **Name and Security Settings** view of the Wizard, enter a name for the new certificate, select a bit length and click **Next**.
12. In the **Organization Information** view of the Wizard, enter an organization name and an OU name. Click **Next**.
13. In the **Your Site's Common Name** view of the Wizard, enter a common name for the Web site. The default will be the host name. Click **Next**.
14. In the **Geographic Information** view of the Wizard, enter the required address information and click **Next**. If sending a request immediately to an online CA, continue at Step 16.
15. In the **Certificate Request File Name** view of the Wizard, enter a name and location path for the certificate request file. Click **Next**. Continue at Step 18.
16. In the **SSL Port** view of the Wizard, make sure the SSL port in the text box is 443 and click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

17. In the **Choose a Certification Authority** view of the Wizard, select the CA from the drop-down menu and click **Next**.
18. In the **Request File Summary** view of the Wizard, click **Next**.
19. To complete the Wizard, click **Finish**.

Notes:

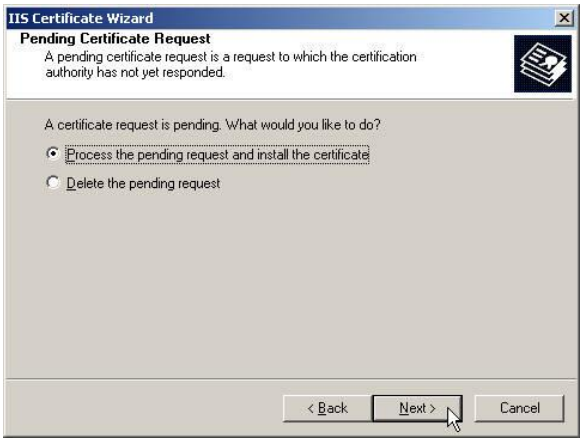
Certificate request files will need to be taken to a CA for processing. Once a certificate is issued by the CA, the certificate will need to be brought back to the Web server host and imported into the Certificates store. Procedures for importing a certificate request to a CA will vary depending on how the CA is managed. Offline CAs are not included in the Windows Server 2003 Certificate Server Evaluated Configuration, but certificates issued by them may be used within the TOE.

Certificate requests that were submitted to an online CA will appear in the Web server host's Certificates store once issued by the CA. For procedures to issue a certificate from a CA, see Appendix B, Windows Server 2003 Certificate Server Evaluated Configuration Administrator's Guide.

Install a Server Certificate and Configure SSL

Finish processing the pending certificate request within IIS to install the certificate to the server, and enable SSL:

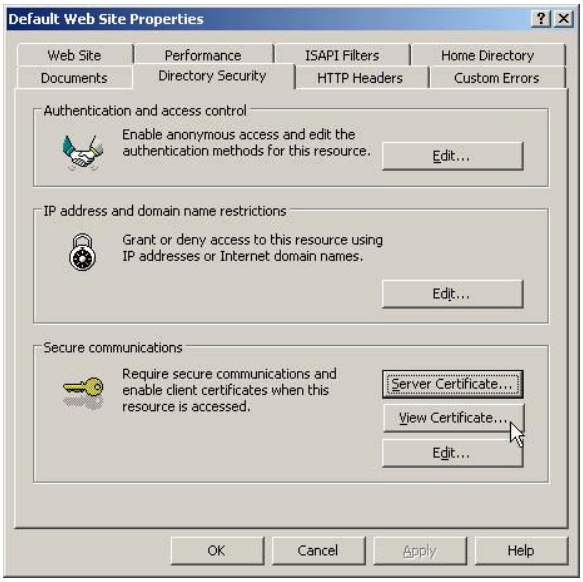
1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. Expand ***Server_name***, where *Server_name* is the name of the server, and then expand **Web Sites**.
4. In the console tree, right-click the Web site or file which is to be protected with SSL, and then select **Properties**.
5. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Server Certificate**.
6. In the **Web Server Certificate Wizard**, click **Next**.
7. Select the **Process the pending request and install the certificate** radio button and click **Next**.



8. Enter the path and file name of the certificate and click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

9. Make sure the correct SSL port is shown (443 by default) and click **Next**. Click **Finish** to complete the wizard. The **View Certificate** button will become active and can be used to view the certificate details.



10. On the **Directory Security** or **File Security** tab, under **Secure communications**, click **Edit**.

11. In the **Secure Communications** interface, select the **Require secure channel (SSL)** check box and click the **Require 128-bit encryption** check box.

12. If desired, enable client certificates by selecting one of the following to enable client Certificate authentication:

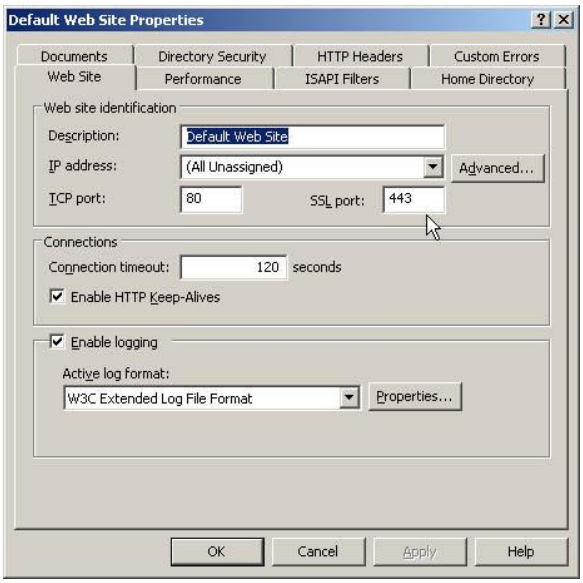
- **Ignore client certificates** - Users with or without a client certificate will be granted access.
- **Accept client certificates** - Users can access the resource with a client certificate, but the certificate is not required.
- **Require client certificates** - The server will request a client certificate before connecting the user to the resource. Users without a valid client certificate will be denied access.

Note: Users attempting to access the Web site can be required to log on with a client certificate. Requiring a client certificate is just one aspect of protecting a server against unauthorized access. Any user with a valid and trusted client certificate will be allowed to establish a secure connection to access the Web resource.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

13. Click **OK**.
14. Click the **Web Site** tab, and make sure that the **SSL Port** text box is populated with the port that is to be designated for SSL. The default (and recommended) port is 443.



15. Click **OK** to close the Web site **Properties** interface.

To test that SSL is enabled, connect to the Web site's homepage by using Secure HTTP (HTTPS):// instead of HTTP://. A valid connection is established if the page appears and there is a small lock icon in the status bar of the Web browser.

Configuring Web Permissions for Web Content

Authorized administrators can set Web permissions for specific Web sites, folders, and files on their Web servers. Unlike the NTFS file system permissions that apply only to either a specific user or a group of users who have a valid Windows account, Web permissions apply to all users who access the Web site regardless of their specific access rights. NTFS permissions control access to physical directories on the server, whereas Web permissions control access to virtual directories on the Web site. When configuring Web permissions, keep the following in mind:

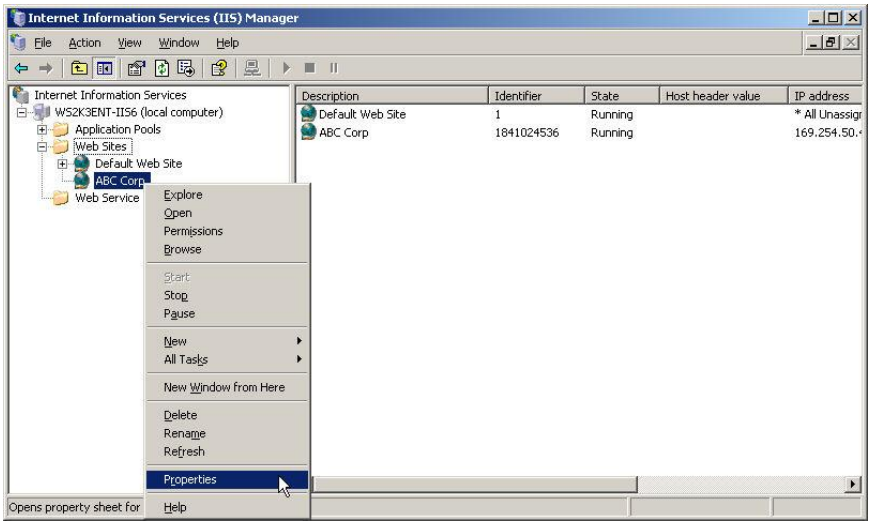
- Web permissions are not meant to replace NTFS permissions; instead, Web permissions should be used with NTFS permissions.
- Unlike NTFS permissions, Web permissions affect everyone that attempts to access the Web site.
- Disabling permissions restricts all users. For example, disabling the **Read** permission restricts all users from viewing a file, regardless of the NTFS permissions applied to those users' accounts. However, enabling the **Read** permission can allow all users to view that file, ***unless*** NTFS permissions that restrict access have also been applied.
- If Web permissions and NTFS permissions differ for either a folder or a file, the more restrictive of the two settings is used. For example, if Write permissions are granted to a folder in IIS, and Read permissions are granted to a particular user group in NTFS, those users cannot write files to the folder because Read permissions are more restrictive.
- When both Web permissions and NTFS permissions are set, the permissions that explicitly deny access take precedence over permissions that grant access.
- To set permissions for a WebDAV directory, keep in mind the following:

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- WebDAV must first be enabled in order to publish in a WebDAV directory.
- Anonymous access to the WebDAV directory must be turned off. Protect the WebDAV directory by using one of the following authentication methods in IIS 6.0, such as Integrated Windows authentication and the DACL in NTFS. For more information about WebDAV security, see "Managing WebDAV Security" in IIS 6.0 Help, which is accessible from IIS Manager.

To configure Web server permissions for Web content, follow these steps:

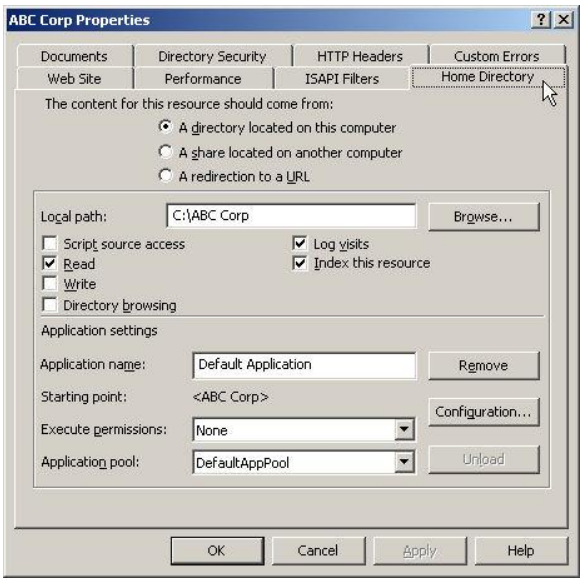
1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. Expand ***ServerName***, where *ServerName* is the name of the server, and then expand **Web Sites**.
4. Right-click either the Web site, the virtual directory, the folder, or the file where permissions are to be set, and then click **Properties**.



5. Select one of the following tabs, as appropriate:
   - **Home Directory**
   - **Virtual Directory**
   - **Directory**
   - **File**
6. Either click to select or click to clear any of the following check boxes (if present) that are appropriate for the level of Web permissions that need to be set:

Copyright © 2008 Microsoft Corporation.

All rights reserved.



- **Script source access**: Grant this permission to permit users to access source code. Source code includes scripts, such as scripts in ASP programs. This permission is only available if either the Read permission or the Write permission is set.

Note: When this option is used, users may be able to view sensitive information, such as a user name and a password, from scripts in an ASP program. They may also be able to change source code that runs on the server. This can seriously affect the security and the performance of the server. Administrators may want to control access to this type of information and to these functions by using individual Windows accounts and higher-level authentication, such as integrated Windows authentication.

- **Read**: Grant this permission to permit users to either view or download files or folders and their associated properties. By default, Read permission is selected.
- **Write**: Grant this permission to permit users either to upload files and their associated properties to the enabled folder on the server or to change the content or properties of a write-enabled file.
- **Directory browsing**: Grant this permission to permit users to view a hypertext listing of the files and the subfolders in the virtual directory. The folder listings do not contain the virtual directories. Users must know the alias of the virtual directory.

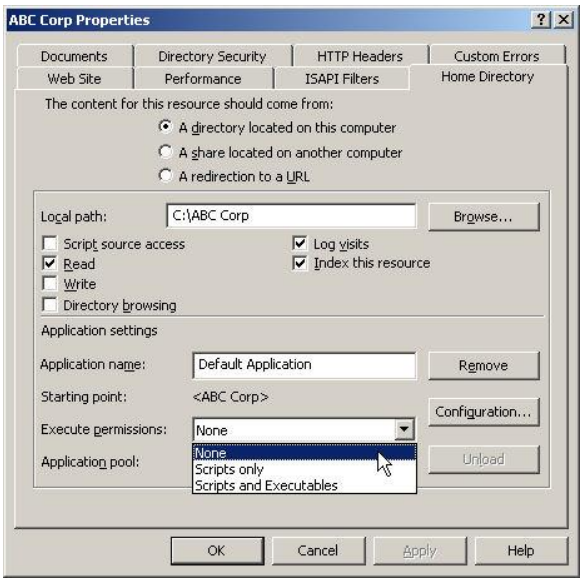
Note: A user may receive an "Access Forbidden" error message if the user tries to access either a file or folder on the server and both of the following conditions are true: (1) directory browsing is disabled; and (2) the user does not specify a file name such as *Filename*.htm in the **Address** box.

- **Log visits**: Grant this permission to log visits to this folder in a log file. A log entry is recorded only if logging is enabled for the Web site.
- **Index this resource**: Grant this permission to permit Microsoft Indexing Service to include this folder in a full-text index of the Web site. When this permission is granted, users can query this resource.

7. In the **Execute Permissions** box, click the desired option to determine how scripts run on the site. T he following options are available:

Copyright © 2008 Microsoft Corporation.

All rights reserved.



- **None:** Click this setting if users are not to run scripts or executable programs on the server. When this setting is used, users can access only the static files such as HTML and image files.
- **Scripts only**: Click this setting to run scripts such as ASP programs on the server.
- **Scripts and Executables**: Click this setting to run both scripts such as ASP programs and executable programs on the server.

8. Click **OK**, and then close the IIS snap-in.

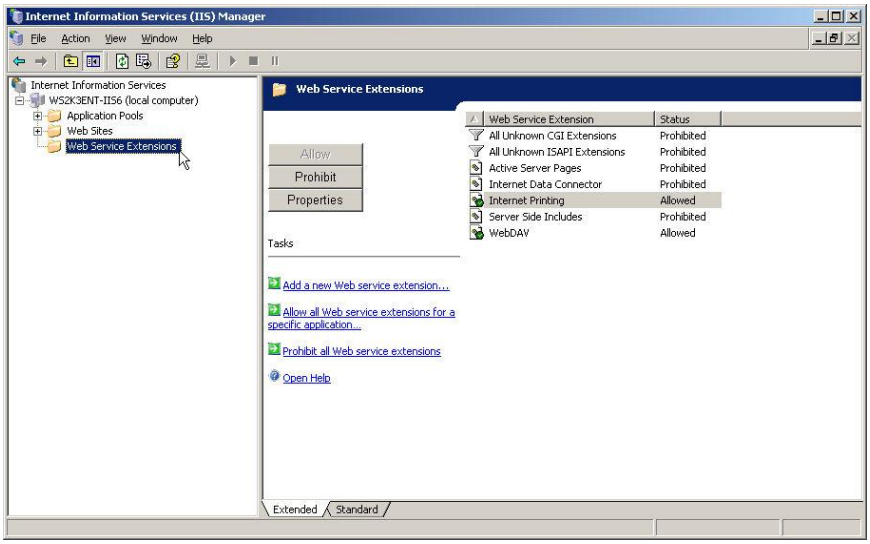
Note: When an attempt is made to change the security properties of a Web site or virtual directory, IIS checks the existing settings on the child nodes (virtual directories and files) that the Web site or virtual directory contain. If the permissions that are set at the lower levels are different, an **Inheritance Overrides** dialog box appears. To specify the child nodes that inherit the permissions that are set at the higher level, click the node or nodes in the **Child Nodes** list, and then click **OK**. The child node inherits the new permissions settings.

Web Service Extensions

By default, IIS 6.0 serves only static content. Features such as ASP, ASP.NET, server-side includes, WebDAV publishing, and FrontPage 2002 Server Extensions from Microsoft do not work unless they are specifically enabled. Authorized administrators can configure these features, also called **Web Service Extensions**, through the Web Service Extensions node in IIS Manager.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

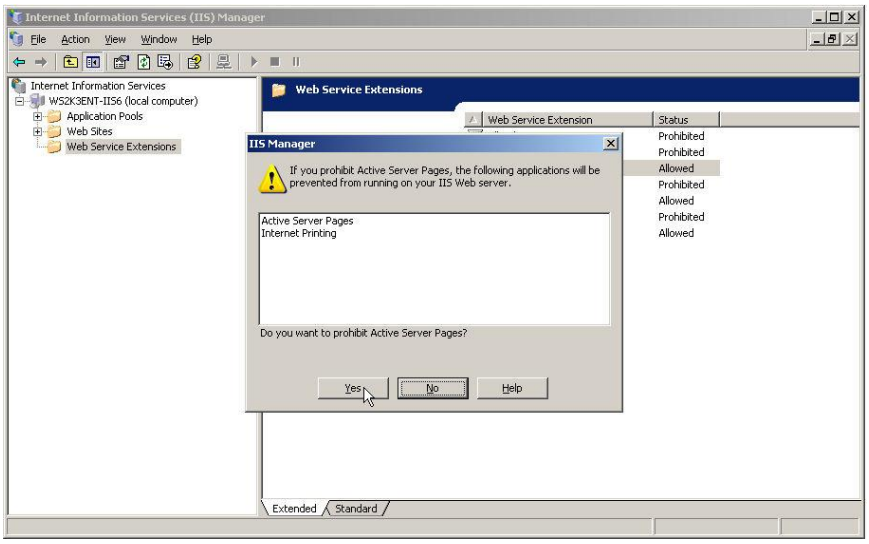


Note: For the Evaluated Configuration, only the **Internet Printing**, **WebDAV**, and **URL Authorization** Web Service Extensions are to be **Allowed**.

Authorized administrators can individually enable or disable a Web service extension if it is registered in the Web Service Extensions node in IIS Manager.

To enable or disable dynamic content:

1. Log on as an authorized administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. Expand ***ServerName***, where *ServerName* is the name of the server, and then select **Web Service Extensions**.
4. In the details pane, select the Web service extension that is to be enabled or disabled.
5. To enable a disabled Web service extension, click **Allow**.
6. To disable an enabled Web service extension, click **Prohibit**. A message box with a list of applications that will be prevented from running on the IIS Web server displays. Click **OK** to disable the Web service extension.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

7. To view the properties of a Web service extension, click **Properties**.

Internet Printing

Internet printing provides the ability to submit print jobs to a printer across the Internet or a local Intranet by allowing users to access printers from a Web page interface:

- Users can install printers by selecting the printer through its URL link name.
- For a computer running a Windows Server 2003 family operating system to process print jobs that contain URLs, it must be running Microsoft IIS.
- Internet printing uses Internet Printing Protocol (IPP) as its low-level protocol, which is encapsulated within HTTP, using it as a carrier. When accessing a printer through a browser, the system first attempts to connect using RPC (on Intranets and LANs), which is fast and efficient.
- Print server security is provided by IIS. To support all browsers and all Internet clients, the authorized administrator must choose basic authentication. Alternatively, the administrator can use Microsoft challenge/response or Kerberos authentication, both of which are supported by Microsoft Internet Explorer.
- Printers may be managed from any browser, however to connect to a printer with a browser, Internet Explorer version 4.0 or higher must be used.

Installing the Internet Printing Component of IIS

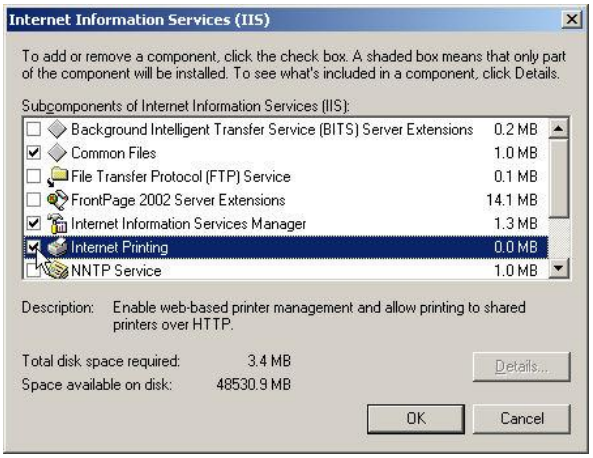
To support **Internet Printing**, the print server must have IIS installed. **Internet printing** should be selected during the installation of IIS as an additional component. To install **Internet Printing** during the IIS installation process, follow the procedures above in Installing IIS 6.0 and make sure to check the **Internet Printing** selection box at step 6.

If **Internet Printing** was not included in the original IIS installation:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.
3. On the **Add or Remove Programs** interface, click the **Add/Remove Windows Components** button to start the **Windows Components Wizard**.
4. In the **Windows Components** list, select the **Application Server** and click the **Details** button.
5. In the **Application Server** interface, select **Internet Information Services (IIS)** and click **Details**.
6. In the **Internet Information Services (IIS)** interface, select the check box for **Internet Printing**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



7. Click **OK** on the **Internet Information Services (IIS)** interface, click **OK** on the **Application Server** interface, and click **Next** on the **Windows Components Wizard** to continue. Click **Finish** to close the Wizard.

Note: ASP will be automatically selected and enabled as a Web Service Extension when Internet Printing is added. For the Evaluated Configuration, it will be necessary to disable ASP as shown above in the Web Service Extensions subsection.

Turn on Internet Printing

Once the **Internet Printing** component is installed with IIS, it should be turned on by default. Authorized administrators may verify that **Internet Printing** is turned on by checking the **Web Service Extensions** list in **IIS Manager**.

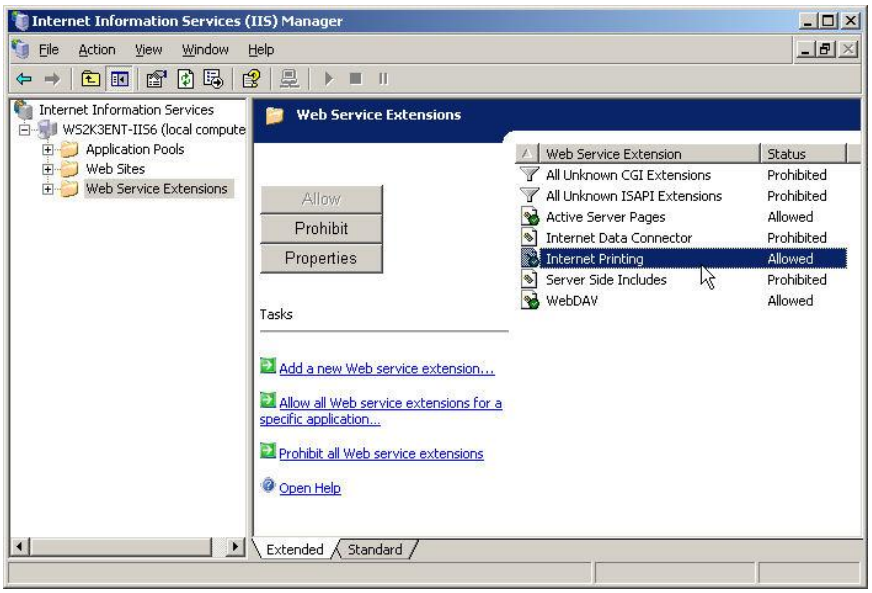
Note: Printers will need to be added to the local host using the **Add Printer Wizard** from the **Printers and Faxes** interface.

To verify that the **Internet Printing** is turned on, or to turn it on:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. Select the **Web Service Extensions** folder and verify that the **Internet Printing** Web Service Extension is set to **Allowed**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

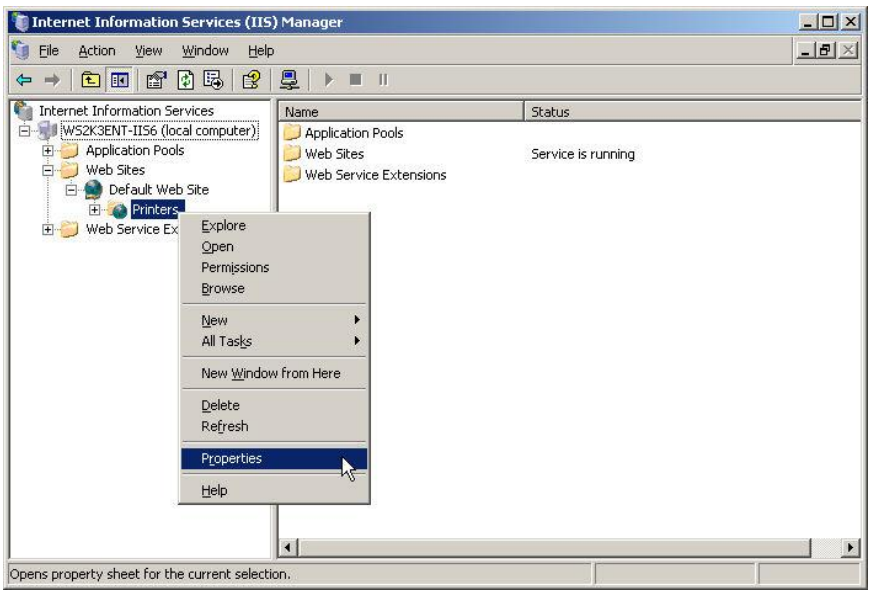


4. If the **Internet Printing** Web Service Extension is shown as **Prohibited**, right-click on **Internet Printing** and select **Allow**.
5. Exit the **IIS Manager**.

Configure the Authentication Method and Access Control for Internet Printing

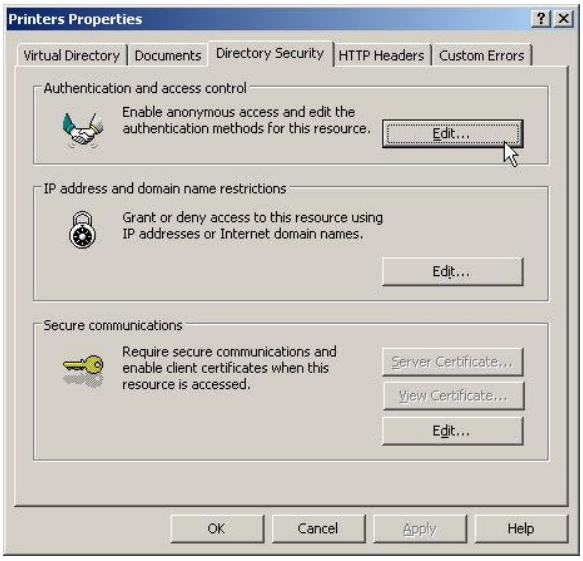
To configure the authentication method for Internet printing, follow these steps:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. Expand **Web Sites**, expand **Default Web Site**, right-click **Printers**, and then click **Properties**.



4. Click the **Directory Security** tab, and then click **Edit** under **Authentication and access control**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

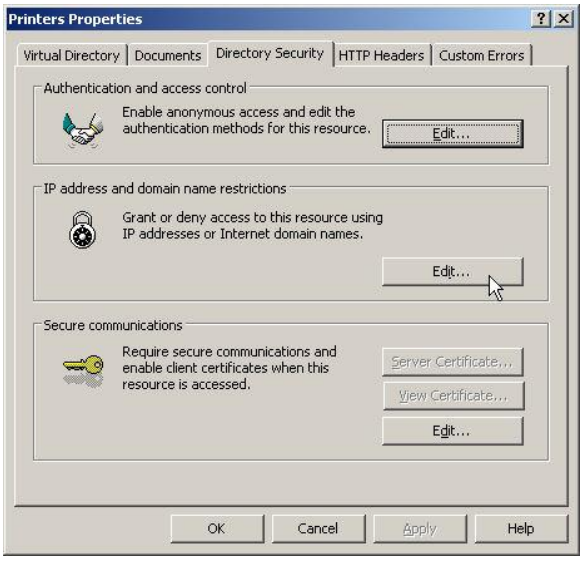


5. See Authentication Based on User Credentials for a description of the authentication options available on the **Authentication Methods** interface.

6. Authorized administrators can also control access to Internet printers based on the requesting host instead of on user credentials. To grant or deny access to specific computers, groups of computers, or domains, click **Edit** under **IP Address and Domain Name Restrictions in the Directory Security tab of the Printers Properties interface**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



7. In the **IP Address and Domain Name Restrictions** dialog box that is displayed, complete one of the following procedures:
   - To explicitly grant access:
     - Select the **Denied Access** radio button to deny access to all computers by default, and then click the **Add button to create exceptions for computers that will be explicitly granted access**.
     - In the **Grant Access On** dialog box, select the desired option and then click **OK**. The computer, group of computers, or domain selected is added to the **Granted** list.
   - To explicitly deny access:
     - Select the **Granted Access** radio button to grant access to all computers by default, and then click **Add button to create exceptions for computers that will be explicitly denied access**.
     - In the **Deny Access On** dialog box that is displayed, specify the desired option and then click **OK**. The computer, group of computers, or domain specified is added to the **Denied** list.
   - Click **OK**.
8. Click **OK**, and then quit **IIS Manager.**

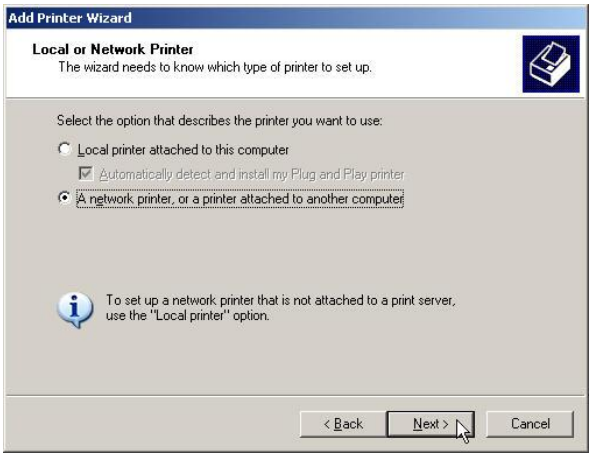
Connect to a Printer Using a URL

To connect to a printer through a URL:

1. Log on as an authorized administrator.
2. Click **Start** and select **Printers and Faxes**.
3. Double-click the **Add Printer** icon.
4. Click **Next** on the **Add Printer Wizard**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

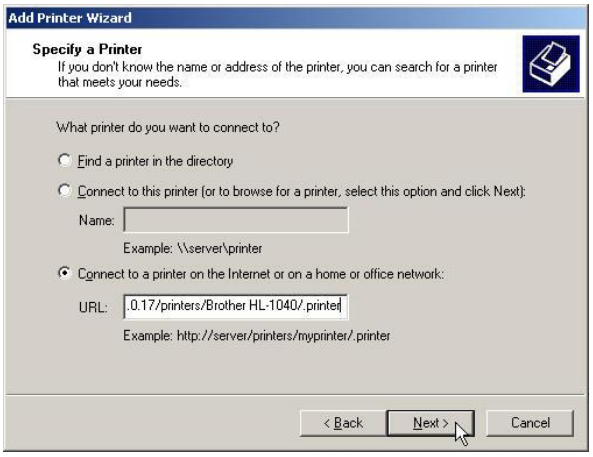
5. Select the "**A network printer, or a printer attached to another computer**" radio button and click **Next**.



6. Select the **Connect to a printer on the Internet or on a home or office network** radio button then enter the URL for the printer. The URL must be entered in the following format:

   http://<name or IP address of server>/printers/<name of printer>/.printer.

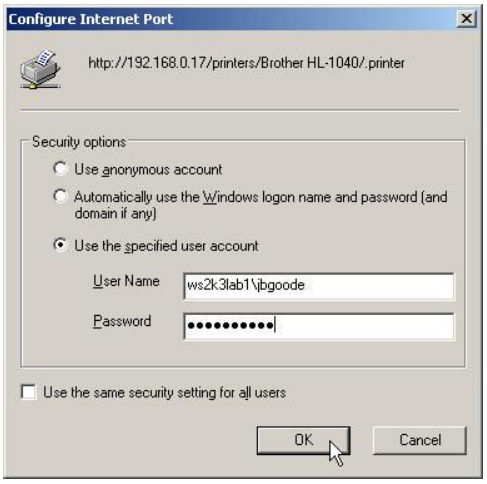
7. Click **Next**.



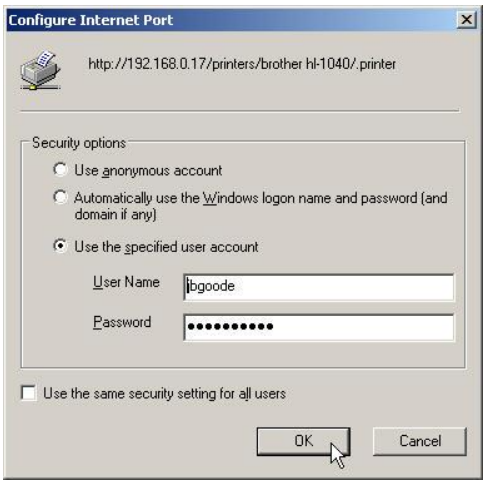
8. A **Configure Internet Port** interface may appear. Select the "**Use the specified user account**" radio button, enter the appropriate user name and password and click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- If the authentication method selected for the Web site is **Windows Integrated Authentication**, enter the user name using the ***<domain name>\<user name>*** format as shown below.



- If the authentication method selected for the Web site is **Digest Authentication**, enter the user name as shown below.



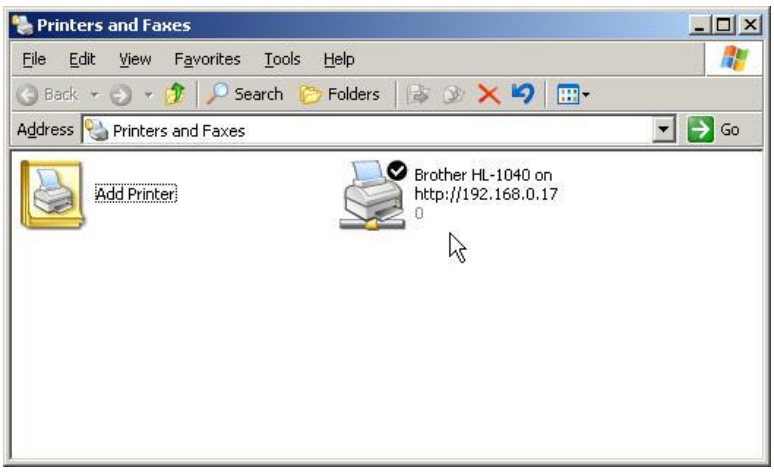
9. Click **Finish** to complete the process of adding the printer. The printer will appear in the **Printers and Faxes** interface.

Note: If this is not the first printer installed on the computer, a **Default Printer** option page will appear prior to this step. Specify whether the printer is to be the default printer and click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

10. The new printer object will appear in the Printers and Faxes interface.



WebDAV

WebDAV extends the HTTP/1.1 to allow clients to publish, lock, and manage resources on the Web. Integrated into IIS, WebDAV allows clients to do the following:

- **Manipulate resources** in a WebDAV publishing directory on a server. For example, users who have been assigned the correct rights can copy and move files around in a WebDAV directory.
- **Modify properties** associated with certain resources. For example, a user can write to and retrieve a file's property information.
- **Lock and unlock resources** so that multiple users can read a file concurrently. However, only one person can modify the file at a time.
- **Search** the content and properties of files in a WebDAV directory.

Setting up a WebDAV publishing directory on a server is as straightforward as setting up a virtual directory through IIS Manager. After setting up a publishing directory, users who have been assigned the correct rights can publish documents to the server and manipulate files in the directory.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

WebDAV Clients

Users access and publish to a WebDAV directory through one of the Microsoft products listed below or through any other client that supports the industry standard WebDAV protocol. For the specific procedure on how to access and publish through these Microsoft products, consult the specific product's Help.

- **Windows clients (Windows Server 2003 and Windows XP):** Connect to a WebDAV directory by adding the directory to the list of Network Places and display the contents as if it were part of the same file system on the local computer. Once connected, users can drag and drop files, retrieve and modify file properties, and complete many other file-system tasks. Users can also connect using the command-line client (known as WebDAV Redirector). This client allows the use of existing applications across the Web and the sharing of files through firewalls and proxy servers.
- **IE (versions 5.0 and 6.0):** Connect to a WebDAV directory by opening the target directory as a Web folder and complete the same file-system tasks as Windows clients.

  Note: IE is not an evaluated component of the Windows Server 2003 Evaluated Configuration.

- **Microsoft Office products (Office 2000 and Office XP):** Create, publish, edit, and save documents directly into a WebDAV directory through any application in Office 2000 or Office XP.

  Note: Microsoft Office products are not included in the Windows Server 2003 Evaluated Configuration.

When enabling WebDAV publishing on an intranet, ensure that all WebDAV clients are running the WebClient service.

WebDav Integrated Security

WebDAV is integrated with the Windows Server 2003 family and IIS, which means WebDAV takes advantage of the security features offered by the platform and the Web server, including permissions control and DACLs in the NTFS file system.

Clients with proper user rights can write to a WebDAV directory, so it is vital to control who accesses the directory. IIS has reinforced Integrated Windows Authentication (formerly called NTLM, and also referred to as Windows NT Challenge/Response authentication) by building in support for the Kerberos V5 security protocol. By selecting Integrated Windows authentication, authorized administrators can make sure that only clients with the correct user rights can access and write to the WebDAV directory on an intranet.

Note: Integrated Windows authentication and Kerberos V5 are not the same thing. Integrated Windows authentication now supports Kerberos V5.

In addition, access to WebDAV directories can be set to require Digest authentication or Advanced Digest authentication.

Installing the WebDAV Publishing Component of IIS

WebDAV Publishing should be selected during the installation of IIS as an additional component. To install **WebDAV Publishing** during the IIS installation process, follow the procedures above in "Installing IIS 6.0" and make sure to check the **WebDAV Publishing** selection box at step 7.

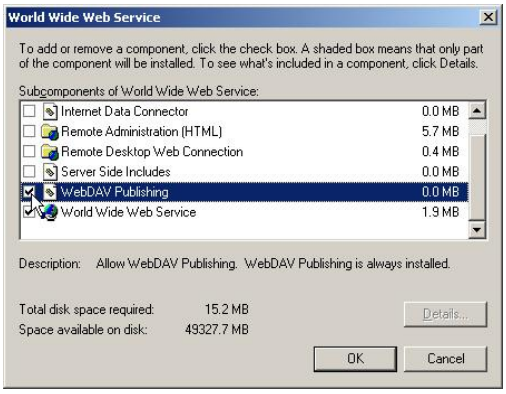
If **WebDAV Publishing** was not included in the original IIS installation:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Control Panel**, and then select **Add or Remove Programs**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

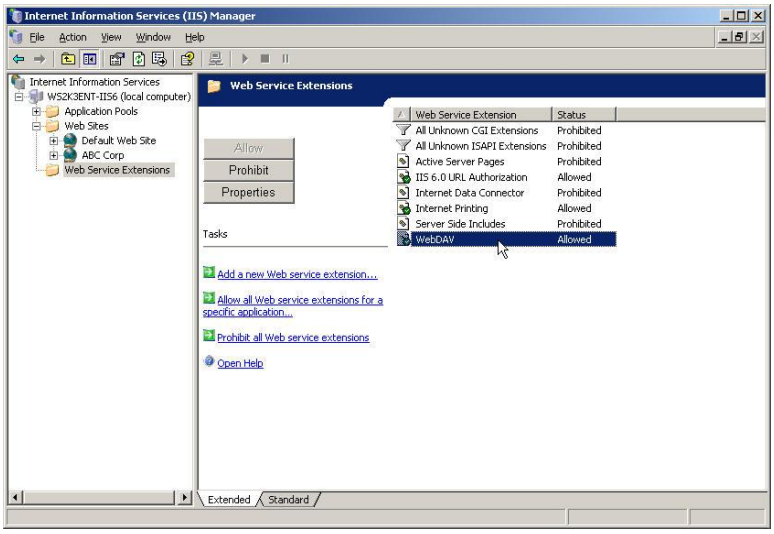
3. On the **Add or Remove Programs** interface, click the **Add/Remove Windows Components** button to start the **Windows Components Wizard**.
4. In the **Windows Components** list, select the **Application Server**, and click the **Details** button.
5. In the **Application Server** interface, select **Internet Information Services (IIS)** and click **Details**.
6. In the **Internet Information Services (IIS)** interface, select **World Wide Web Service** and click **Details**.
7. In the **World Wide Web Service** interface, check the box next to **WebDAV Publishing**.



8. Click **OK** on the **World Wide Web Service** interface, click **OK** on the **Internet Information Services (IIS)** interface, click **OK** on the **Application Server** interface, and click **Next** on the **Windows Components Wizard** to continue. Click **Finish** to close the Wizard.

Enable the WebDAV Web Service Extension in IIS Manager

1. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
2. Select the **Web Service Extensions** folder and verify that the **WebDAV** Web Service Extension is set to **Allowed**.



3. If the **WebDAV** Web Service Extension is shown as **Prohibited**, right-click on **WebDAV** and select **Allow**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

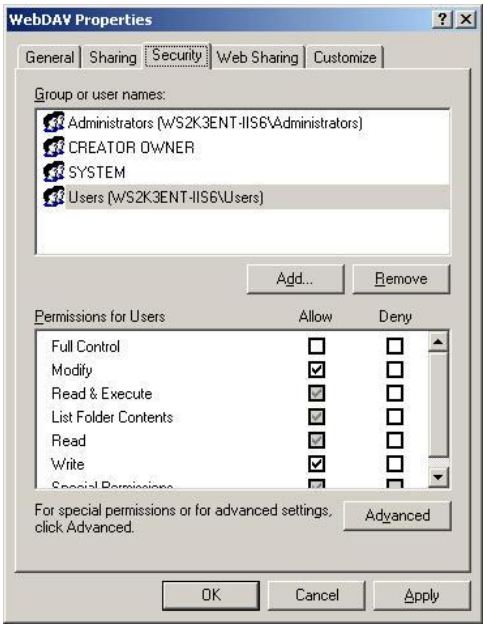
4. Exit the **IIS Manager**.

Creating WebDAV Publishing Directories

Before setting up a WebDAV publishing directory, ensure that the publishing directory resides in an NTFS partition and be sure the WebDAV extension is enabled in **IIS Manager**.

WebDAV publishing and file management requires the following permissions for users on the NTFS directory:

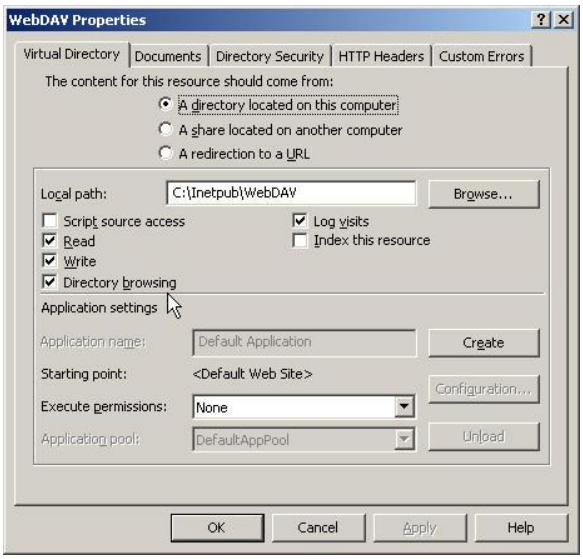
- **Read**: Enables users to read the contents of a file.
- **List**: Enables users to view the contents of the directory.
- **Write**: Enables users to access and change the source of a script and to publish files.
- **Modify**: Enables users to rename or delete a directory or file.



WebDAV publishing and file management requires the following permissions for users on the IIS virtual directory:

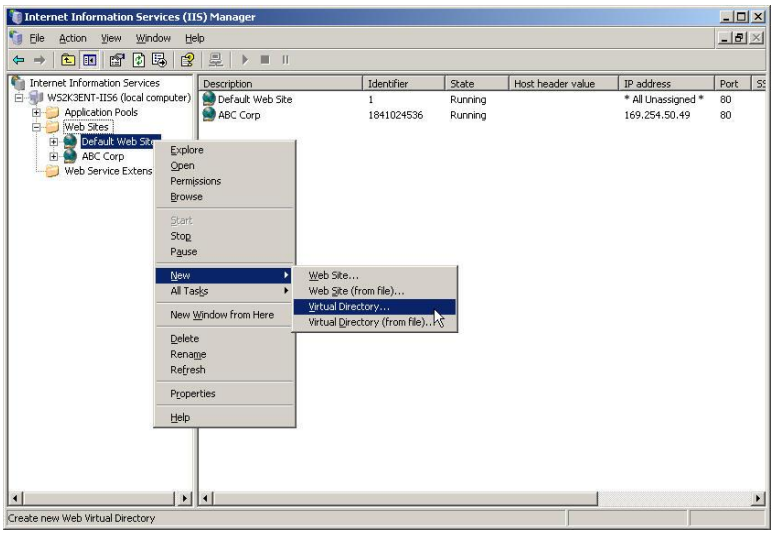
- **Read**: Enables users to read the contents of a file.
- **Directory Browsing**: Enables users to view the contents of the directory.
- **Write**: Enables users to access and change the source of a script and to publish files.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



To set up a publishing directory:

1. Log on as an authorized administrator.
2. Create a directory on the Web server and set the desired NTFS permissions. The directory can be created anywhere on the Web server. For example, if the directory name is WebDAV, the path to this directory can be C:\Inetpub\WebDAV. This directory can be placed anywhere except under the Wwwroot directory. Wwwroot is an exception because its default DACLs are different from those on other directories.
3. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**. Select a Web site in which to create the virtual directory. For this example, we select the Default Web Site.
4. Right-click on the Web site, point to **New**, then select **Virtual Directory**.



5. Follow the directions of the **Virtual Directory Creation Wizard** to create a virtual directory, and then map it to the physical directory that was created above in step 2. Type **WebDAV** as the alias for this virtual directory.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

6. Reset the default NTFS file system permissions to something more restrictive. Users need at least Read permissions to see the directory. If users want to upload content, users also need Write permissions.
7. Grant the Read, Write, and Browsing access permissions for the virtual directory from the **IIS Manager**. This grants users the right to publish documents on this virtual directory and to see a list of the files in it.

Note: Granting Write access does not give a client the ability to modify script-mapped files. To allow these files to be modified, authorized administrators must grant Write permissions and Script source access after creating the virtual directory.

After setting up a WebDAV virtual directory, clients can be allowed to publish to it.

Authenticating Clients

The best way to configure a WebDAV directory depends on the kind of publishing that is desired. When a virtual directory is created through IIS, Anonymous and Integrated Windows authentication are both turned on. Anonymous authentication must not be allowed for access to a WebDAV directory in the Evaluated Configuration. Without controlling who has access, a directory could be attacked by unknown clients. For a description of the authentication options available for a virtual directory, see Authentication Based on User Credentials.

Controlling Access

This section describes how to control access to a WebDAV directory by coordinating IIS and Windows Server 2003 permissions, and how to protect script files.

Configuring Web Permissions

The following are various ways to configure Web permissions based on the purpose of the material to be published:

- **Read, Write, and directory browsing enabled**: Turning on these permissions allows clients to see a list of resources, modify them (except for those resources without Write permission), publish their own resources, and manipulate files.
- **Write enabled; and Read and directory browsing disabled**: If clients are to be allowed to publish private information on the directory, but others are not to see what has been published, set Write

Copyright © 2008 Microsoft Corporation.
All rights reserved.

permission and do not set Read or directory browsing permission. This configuration works well if clients are submitting ballots or performance reviews.

- **Read and Write enabled; and directory browsing disabled**: Set this configuration if to rely on obscuring file names as a security method. However, be aware that security by obscurity is a low-level security precaution because an attacker could guess file names by trial and error.
- **Index this resource enabled**: The Indexing Service is used to let clients search directory resources.

Note: The Indexing Service is not enabled in the Evaluated Configuration.

Controlling Access with DACLs

WebDAV takes advantage of the security features offered by the platform and the Web server, including permissions control and DACLs in the NTFS file system. When setting up a WebDAV publishing directory on an NTFS file system drive, make sure the **Everyone** group has Read permission only. Then assign Write permission to specific individuals or groups.

Protecting Script Code

If there are script files in the publishing directory that are not to be exposed to clients, access to these files can be denied by verifying that **Script source access** permission is *not* assigned. Executable files are treated as static HTML files unless **Scripts and Executables** is enabled for the directory.

To prevent .exe files from being downloaded and viewed as HTML files, but to allow .exe files to run, on the **Virtual Directory** property sheet of the publishing directory, change the Execute Permissions to **Scripts and Executables**.

This level of permission makes all executable files subject to the **Script source access** setting. When **Script source access** is selected, clients with Read permission can see all executables; and clients with Write permission can edit them, as well as run them.

With the following permissions, clients can write to an executable file that does not appear in the Application Mapping:

- Write permission is assigned.
- Execute Permissions is set to **Scripts only**.

With the following permissions, clients can write to any executable file, regardless of whether it appears in the Application Mapping:

- **Script source access** is assigned.
- Execute Permissions is set to **Scripts and Executables**.

Enabling the WebClient Service

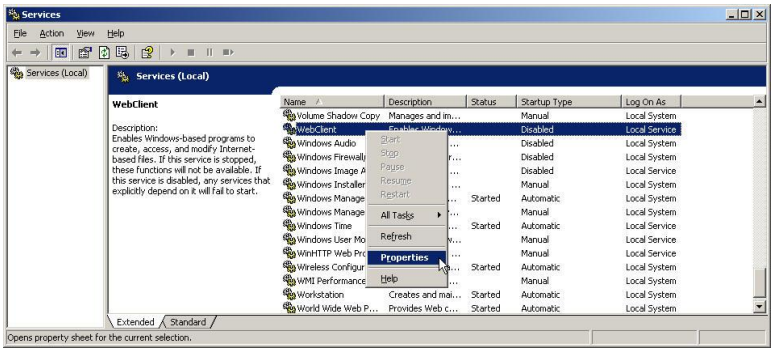
In order to access WebDAV directories, clients will need to have the **WebClient** service enabled. The WebClient service is installed by default on all Windows XP Professional and Windows Server 2003 clients, but is disabled. To enable the WebClient service on a Windows Server 2003 client:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Services**.
3. Scroll through the list of services in the details pane to find and select the **WebClient** service.

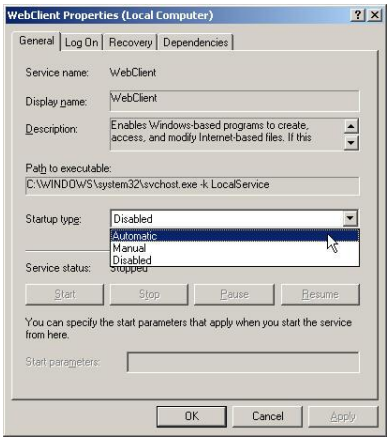
Copyright © 2008 Microsoft Corporation.

All rights reserved.

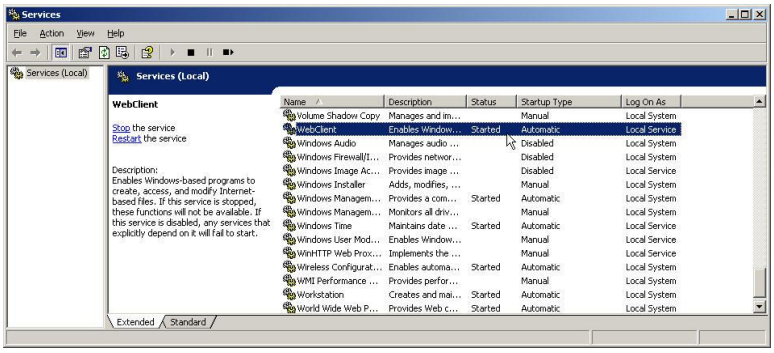
4. Right-click on the **WebClient** service and select **Properties**.



5. Change the **Startup type** to **Automatic** and click **Apply**.



6. Click the **Start** button to start the service. Click **OK** to close the **Properties** interface.

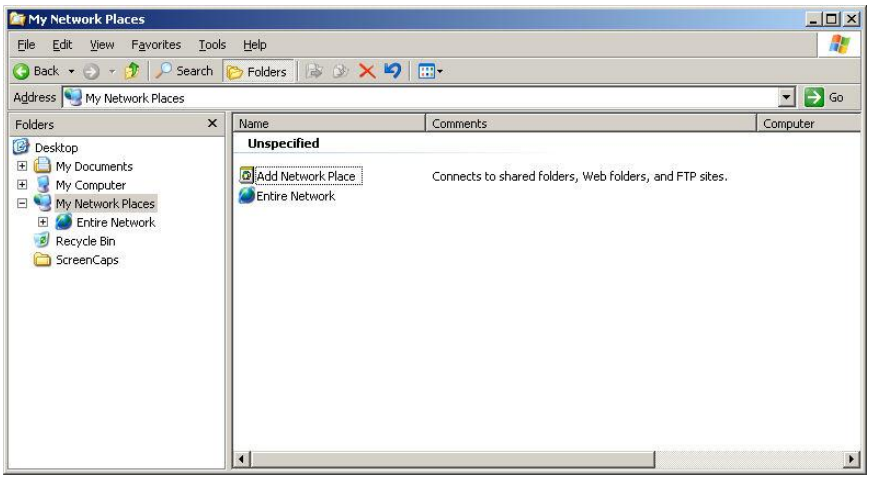


Connecting to a WebDAV Directory

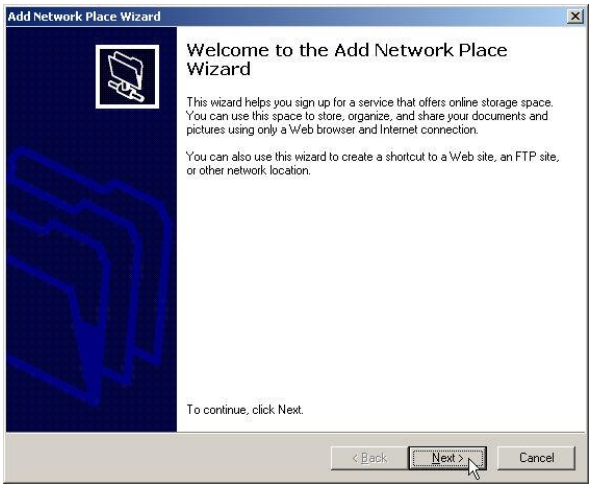
Users can connect to a WebDAV directory by adding a network share in **My Network Places**.

1. On a Windows Server 2003 client, click **Start** and select **Windows Explorer**.
2. In **Windows Explorer**, select **My Network Places**.

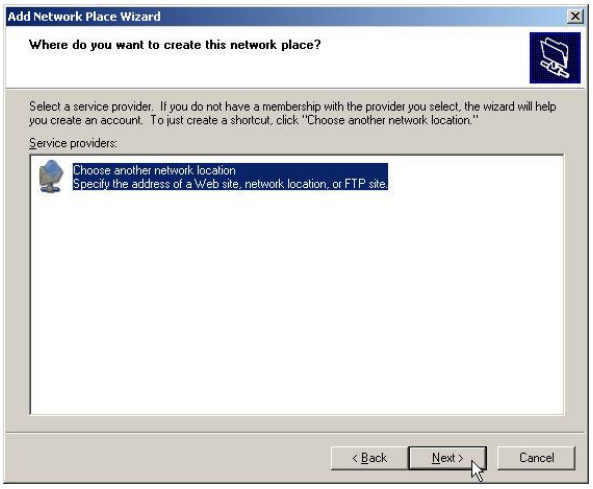
Copyright © 2008 Microsoft Corporation.
All rights reserved.



3. Double-click on the **Add Network Place** icon to start the **Add Network Place Wizard**. Click **Next**.

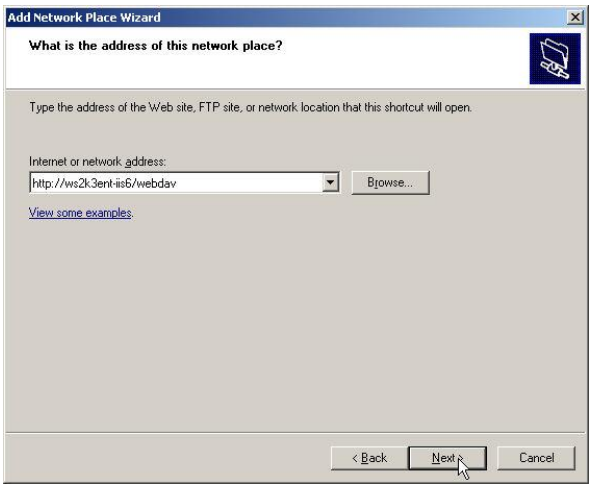


4. Select **Choose another network location** and click **Next**.



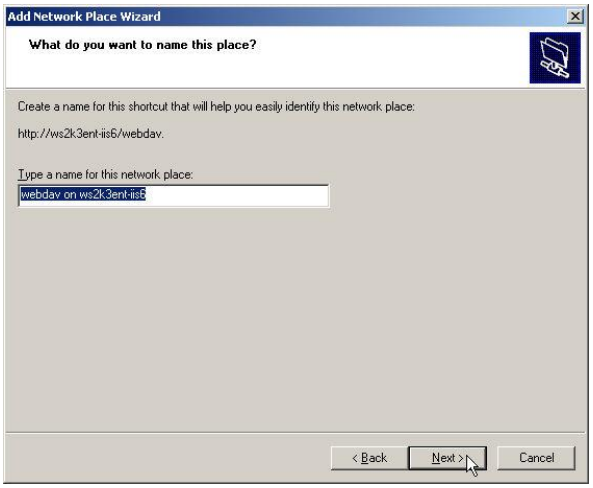
5. In the **Internet or network address** text box, enter the network path to the WebDAV folder. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



6. Depending on the type of authentication requirements set for the WebDAV folder, an authentication request may appear. Enter the appropriate account and password information and click **OK**.

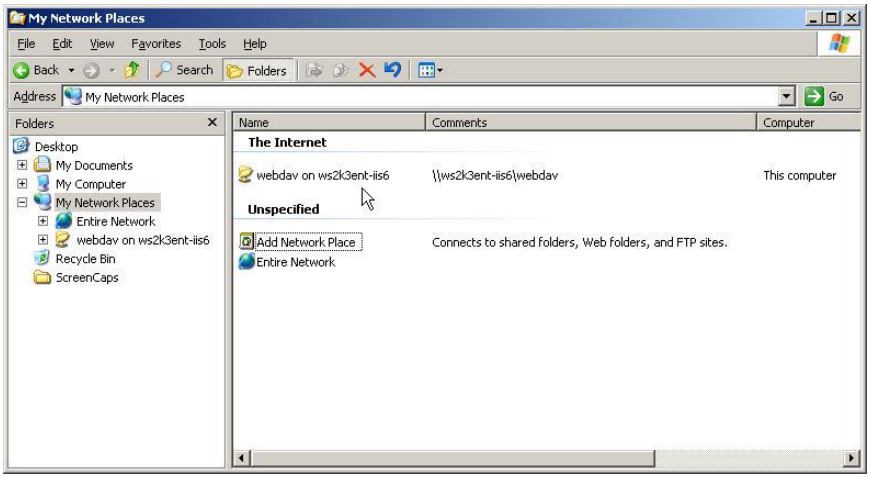
7. Enter a name for the network place, or accept the default, then click **Next**.



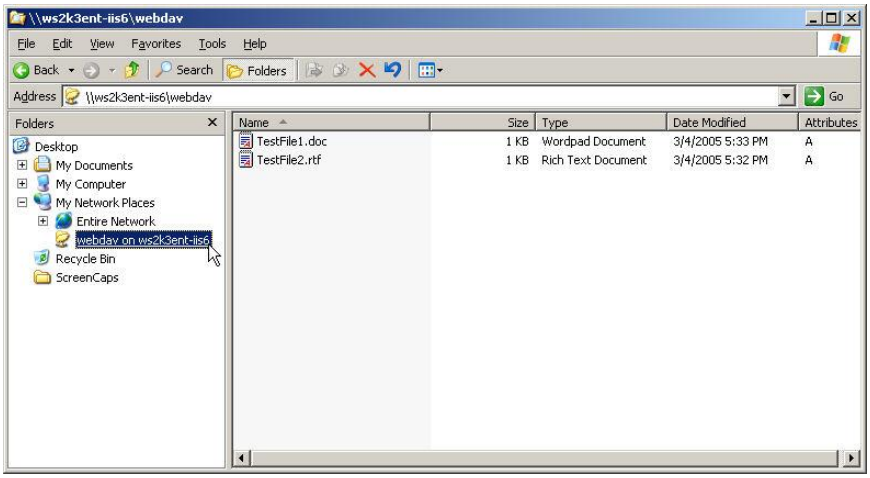
8. Click **Finish** to complete the Wizard.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

9. A network folder, mapped to the WebDAV folder, will appear in **Windows Explorer**.



10. The folder may be accessed in the same manner as any other folder in windows explorer and access to the contents will be based on virtual directory and NTFS permissions specified for the WebDAV site and its folder contents.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

Remote EFS Operations on File Shares and Web Folders (WebDAV folders)

Users can encrypt and decrypt files that are stored on network file shares or on WebDAV Web folders. Web folders have many advantages compared to file shares, and Microsoft recommends the use of Web folders whenever possible for remote storage of encrypted files. Web folders require less administrative effort and are more secure than file shares. Web folders can also securely store and deliver encrypted files over the Internet by using standard HTTP file transfers. Using file shares for remote EFS operations within the Evaluated Configuration requires a Windows Server 2003 domain environment because EFS must impersonate the user by using Kerberos delegation to encrypt or decrypt files for the user.

The primary difference between remote EFS operations on files stored on file shares and files stored on Web folders is where the operations occur. When files are stored on file shares, all EFS operations occur on the computer on which the files are stored. For example, if a user connects to a network file share and chooses to open a file that he or she previously encrypted, the file is decrypted on the computer on which the file is stored and then transmitted in plaintext over the network to the user's computer. When files are stored on Web folders, all EFS operations occur on the user's local computer. For example, if a user connects to a Web folder and chooses to open a file that he or she previously encrypted, the file remains encrypted during transmission to the user's computer and is decrypted by EFS on the user's computer. This difference in where EFS operations occur also explains why file shares require more administrative configuration than Web folders.

Remote EFS Operations in a Web Folder Environment

When users open encrypted files stored on Web folders, the files remain encrypted during the file transfer, and EFS decrypts them locally. Both uploads to and downloads from Web folders are raw data transfers, so even if an attacker could access the data during the transmission of an encrypted file, the captured data would be encrypted and unusable.

EFS with Web folders eliminates the need for specialized software to securely share encrypted files between users, businesses, or organizations. Files can be stored on common intranet or Internet file servers for easy access while strong security is maintained by EFS.

The WebDAV redirector is a mini-redirector that supports the WebDAV protocol, an extension to the HTTP 1.1 standard, for remote document sharing over HTTP. The WebDAV redirector supports the use of existing applications, and it allows file sharing across the Internet (for example, using firewalls, routers) to HTTP servers.

Users access Web folders in the same way that they access file shares. Users can map a network drive to a Web folder by using My Computer. Upon connecting to the Web folder, the user can choose to copy, encrypt, or decrypt files exactly as they would by using files on file shares.

Note: Web folders are not included in browse lists. To connect to a Web folder, the user must specify the full path (for example, \\ServerName\WebShareName).

Remote Encryption of Files on Web Folders

When a user chooses to encrypt a file on a Web folder, the file is automatically copied from the Web folder to the user's computer, encrypted on the user's computer, and then returned to the Web folder. The advantage to this is that the computer hosting the Web folder does not need to be trusted for delegation and does not require roaming or remote user profiles. No other administrative tasks beyond creating the Web folder and assigning user permissions are required. The disadvantage is that the file must be transmitted from the Web folder to the local computer in order to be encrypted. Organizations need to consider whether the bandwidth requirements for Web folders outweigh the administrative effort necessary to maintain file shares for encrypted file storage. It must also be considered that Web folders are not recommended for files over 60 MB in size.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: Bandwidth requirements are reduced and greater security is ensured if the user first encrypts the file locally and then stores the file on the Web folder. The encrypted file is transmitted in ciphertext when it is transmitted to a Web folder.

Remote Decryption of Files on Web Folders

When a user chooses to decrypt a file on a Web folder, the file is automatically copied from the Web folder to the user's computer in ciphertext. EFS then decrypts the file on the user's computer. If the user opens the encrypted file for use in an application, the file is never decrypted anywhere except on the user's computer. If the user chooses to decrypt a file on the Web folder rather than on the local computer, the file is transmitted in plaintext and stored in plaintext on the Web folder after it is decrypted on the user's computer. The computer hosting the Web folder does not require any configuration except for the creation of the Web folder and the assigning of user permissions in order for remote decryption to function.

File Copy from a Web Folder

Encrypted files are copied from Web folders in the same way that plaintext files are copied from file shares. The file is transmitted in ciphertext and remains encrypted on the local computer if possible. The encryption status for files copied from Web folders is the same as that for files copied locally. For more information about encryption status for copied files see Copying an Encrypted Folder or File.

IIS 6.0 URL Authorization

Authorizing user access to Web application resources requires the management of many ACLs. In turn, maintaining ACLs requires administrators to track precisely which permissions are needed on each resource for each user or group to perform meaningful tasks. IIS URL authorization allows authorized administrators to simplify access management by authorizing user access to the URLs that comprise a Web application.

When a user requests access to a URL, IIS URL Authorization validates the user's access based on that user's roles, which can be defined in LDAP queries, custom user roles, and **Authorization Manager** scripts (BizRules). This allows authorized administrators to simplify access control management by controlling all user access to URLs instead of controlling access per ACL on each resource.

Note: For details on using dynamic business rules in Windows Server 2003 Authorization Manager see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetserv/html/AzManBizRules.asp.

IIS 6.0 URL Authorization is implemented as an Internet Server API (ISAPI) interceptor DLL (Urlauth.dll) that is configured as a wildcard extension for a program, for a virtual directory, or for a URL. When an application, virtual directory, or URL is configured to use IIS URL authorization, each request to a URL will be routed to the IIS 6.0 URL authorization ISAPI interceptor. The URL authorization ISAPI interceptor will use **Authorization Manager** to authorize access to the requested URL. The URL must be associated with an **Authorization Manager** policy store that contains the authorization policy for the URL. Once the client has been authorized to access the URL, the URL authorization ISAPI's Execute URL feature will pass the request to the appropriate handler for the URL, such as another ISAPI or the Static File Handler.

IIS 6.0 URL Authorization can be used to control access based on information that is only available at run time. For example, if there is a Web page that only employees in a specific cost center or employees of a specific age should be able to view, roles can be assigned to the correct users based on LDAP queries. The LDAP queries verify the cost center attribute or the age attribute on a user object at run time. If employees can be allowed to access some pages only on specific days of the week or only during a

Copyright © 2008 Microsoft Corporation.

All rights reserved.

specific time of day, an Authorization Manager script can be created that grants access to the URL based on these values. An Authorization Manager script can be created for any value that can be asserted at run time, including IIS Server Variables.

IIS 6.0 URL Authorization uses the metabase attributes in the following table to set authorization on a URL, on a virtual directory, or on a program.

Attribute	Authorization
AzEnable	This attribute enables IIS 6.0 URL Authorization for the virtual directory, for the program, or for the URL that corresponds to the entry in the metabase.
AzStoreName	This attribute associates an Authorization Manager store with the virtual directory, the program, or the URL.
AzScopeName	This attribute associates the virtual directory, the program, or the URL with a scope that the **AzStoreName** attribute refers to in the Authorization Manager policy store in IIS 6.0 URL Authorization. If this attribute specifies either an empty string or no scope at all, the default scope of IIS 6.0 URL Authorization is used.
AzImpersonate	This attribute determines the impersonation behavior for the program. This attribute can be used to configure the Web program to impersonate the client user, the IIS worker process, or the IUSER_* account for the worker process. Each setting significantly changes the environment and the implied design of the Web program. Set the value to **0**, to **1**, or to **2**. These values correspond to the impersonation style. **0** The authenticated client is impersonated. Use this value to use IIS 6.0 URL Authorization for programs that expect to run while impersonating the client, such as ASP 2.0 programs. **Note:** ASP is not included in the Evaluated Configuration. **1** The IIS worker process identity is impersonated. Use this value when the program runs as a service account, authorizes each client request itself, and performs requested operations on behalf of the client in the trusted service context. **2** The anonymous user account is impersonated. Use this value to configure IIS 6.0 URL Authorization to authorize client access to the URL while still running the Web program as the anonymous account. This configuration limits all client access through the Web program.

Sample Script

The sample script below, written in Microsoft Visual Basic Scripting Edition, uses Active Directory Service Interfaces (ADSI) to set the metabase attributes on the IIS metabase entry for a program, for a virtual directory, or for a URL. The script assumes that an IIS virtual directory has been created that corresponds to the script. Use of this script is demonstrated later in **Configure the IIS Metabase to Use IIS URL Authorization for the Web Program**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

```
' SetUrlAuth.vbs
' Configuring UrlAuth with a virtual directory
' This script uses ADSI to configure a virtual directory in the IIS 6.0 metabase to use
' IIS 6.0 URL Authorization.
'
' This script assumes that you have already created the IIS virtual directory
'  that corresponds to the program.
'
' After you run this script to verify the settings, use the Adsutil tool in
' the following way:
'
' inetpub\adminscripts\adsutil enum w3svc/1/root/MyApp
' (where MyApp is the application name)
' Use the Authorization Manager MMC snap-in to:
'    Create an application that is named IIS 6.0 URL Authorization.
'    Create an operation that is named AccessURL and that has an operation ID of 1.
'    Create a scope that corresponds to the AzScopeName that is specified to this script.
'      This scope name is used to manage access to URLs in this virtual directory.
'    Make sure that the IIS worker process has read access to the
'      AzMan policy store. To do this, right-click the AzMan store, click Options,
'      and then click the Security tab.
Set objArgs = WScript.Arguments
If objArgs.count < 4 then
  wscript.echo "Usage: SetUrlAuth VDirPath AzScopeName AzStoreName AzEnable [ImpersonationLevel]"
  wscript.echo ""
  wscript.echo "Example:"
  wscript.echo " SetUrlAuth w3svc/1/root/MyApp MyApp msxml://d:\inetpub\wwwroot\AzStore.xml True 1"
  wscript.echo ""
  wscript.echo "Run with 'cscript' command in cmd.exe to avoid msg boxes"
Else
wscript.echo objargs(0)
'
' Get the interface to the virtual directory object.
'
DIM iis
set iis = GetObject("IIS://localhost/" & objArgs(0))
' Set the scope name. This scope will preside over URLs that refer to this virtual directory.
```

Copyright © 2008 Microsoft Corporation.
All rights reserved.

```
' This scope must exist in the corresponding Authorization Manager store.
'
iis.AzScopeName = objArgs(1)
'
' Specify location of Authorization Manager policy store
'
iis.AzStoreName = objArgs(2)
'
' Enable IIS 6.0 URL Authorization for this virtual directory.
'
iis.AzEnable = objArgs(3)
'
' Set the Impersonation Level property.
'
If objArgs.count > 4 then
  iis.AzImpersonationLevel = objArgs(4)
End if
'
' Write the settings to the metabase.
'
iis.SetInfo
End if
```

When IIS 6.0 URL authorization is configured, the **AzStoreName** attribute in the IIS metabase entry for the application, virtual directory, or URL will identify an **Authorization Manager** policy store. To manage the authorization policy, run **Authorization Manager** and use the **Open Policy Store**. IIS 6.0 URL authorization is an application in this store. The **AzScopeName** attribute in the metabase entry will be an authorization manager scope in the IIS 6.0 URL authorization application. Use this scope to manage access to the corresponding URL. When configuring an application, virtual directory, or URL for URL authorization, a scope must be created in the authorization policy store with the same name as that specified in the corresponding metabase entries **AzScopeName** attribute.

Configuring URL Authorization

This subsection describes how to set up IIS 6.0 URL Authorization for a Web program by using an example URL. The example URL is named WebApp and is installed and configured in IIS as a program in the %Systemroot%\InetPub\WWWroot\WebApp folder. The procedures in this subsection were derived from Microsoft Knowledge Base Article 326020, *How to configure IIS 6.0 URL Authorization* (http://support.microsoft.com/default.aspx?scid=kb;en-us;326020#1).

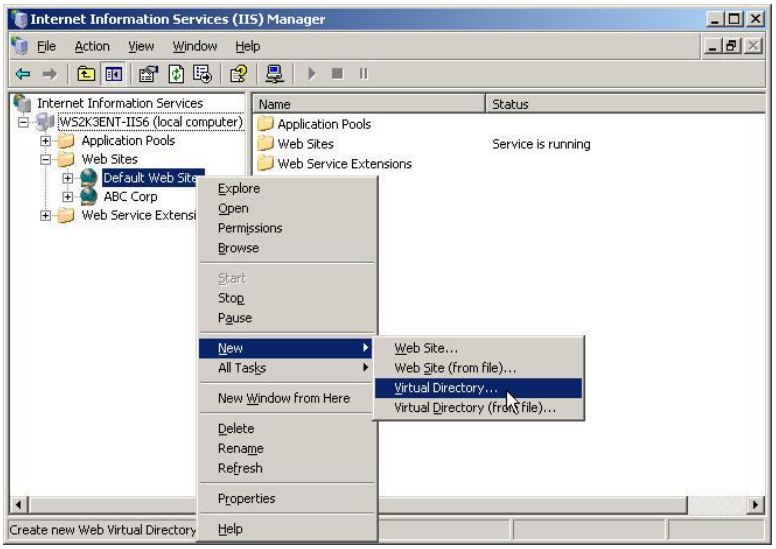
Note: Integrated Windows Authentication is required for URLs that use IIS 6.0 URL Authorization. By default, IIS Web programs and virtual directories turn on Integrated Windows Authentication.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Step 1 - Create a program folder under the Default Web Site folder and disable anonymous access

1. Log on as an authorized administrator.
2. For this example, create the %Systemroot%\InetPub\WWWroot\WebApp folder, if it does not already exist.
3. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
4. In the console tree, expand **Internet Information Services**, double-click the name of the computer that is running IIS, expand **Web Sites**, right-click **Default Web Site**, point to **New** and select **Virtual Directory**.

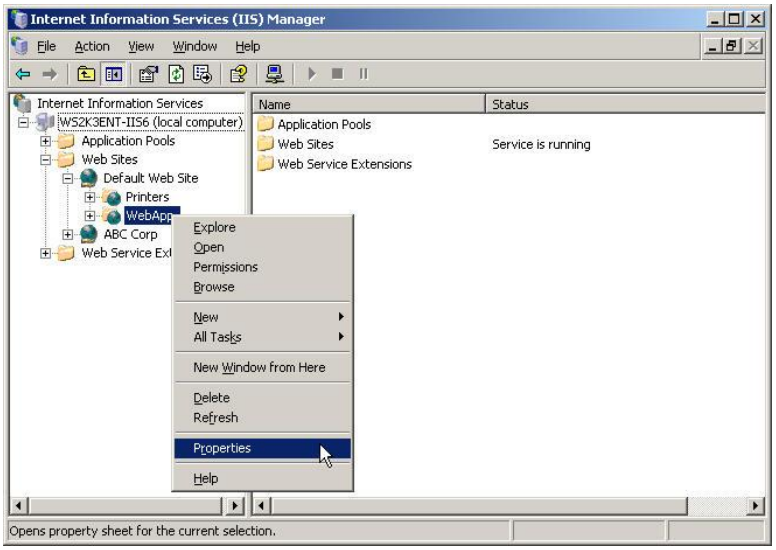


5. Follow the **Virtual Directory Creation Wizard** to create the new virtual directory folder. For this example, the virtual directory will be called WebApp.

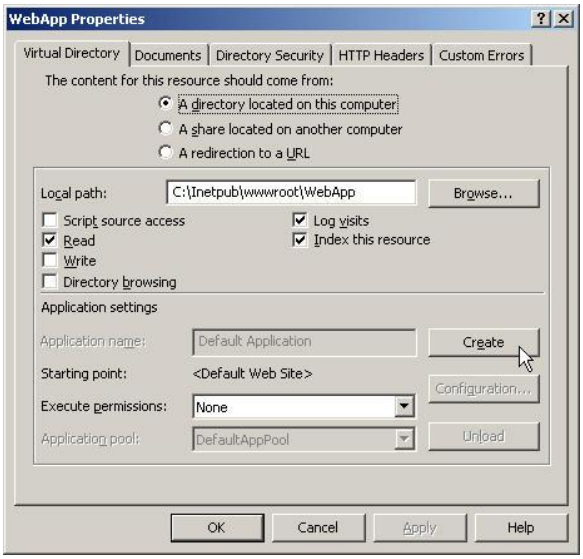
6. In **IIS Manager**, right-click the folder that corresponds to the Web program (in this example, the WebApp folder) and then select **Properties**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



7. Click the **Virtual Directory** tab, and then click **Create**. The folder name will appear in the **Application name** text box (in this example, WebApp).

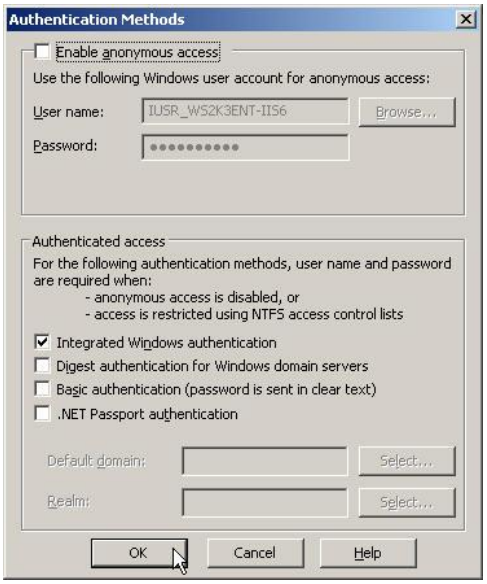


8. Click the **Directory Security** tab, and then click **Edit** in the **Authentication and Access Control** area.

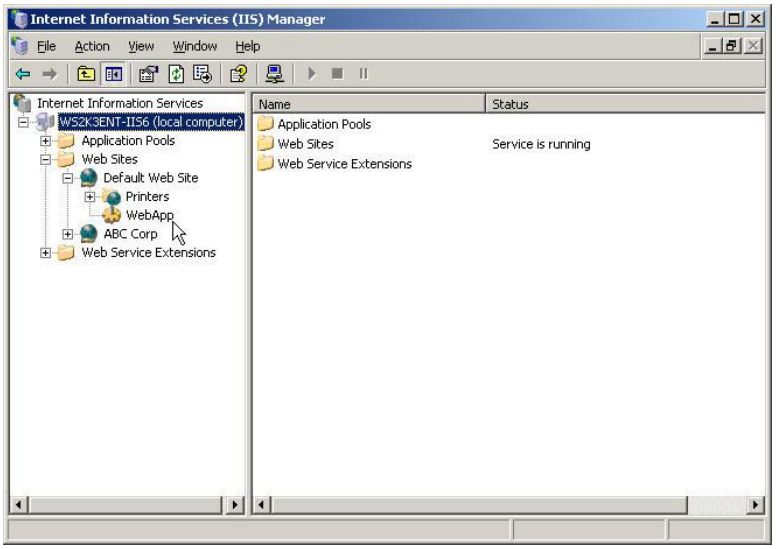
9. Click to clear the **Enable Anonymous Access** check box. Click to select the **Integrated Windows Authentication** check box, click **OK**, and then click **OK** again.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



10. The folder icon will change to indicate a program folder.

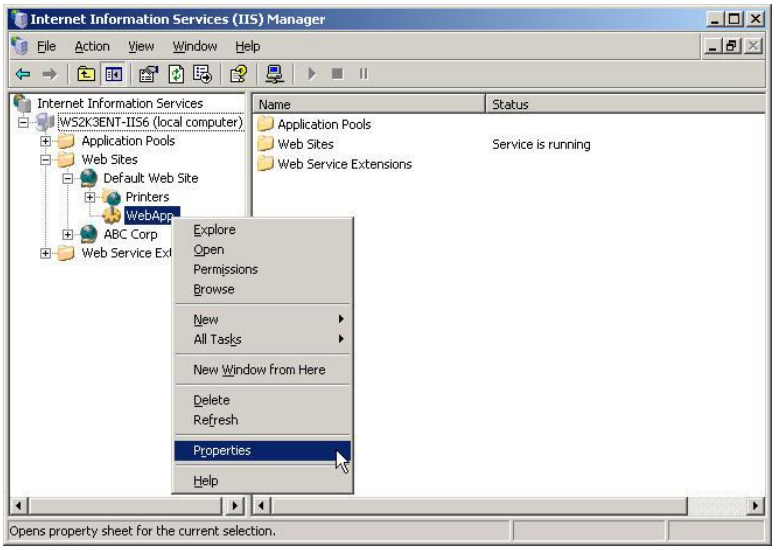


Step 2 - Set the wildcard configuration properties to point to the URLAuth.dll file

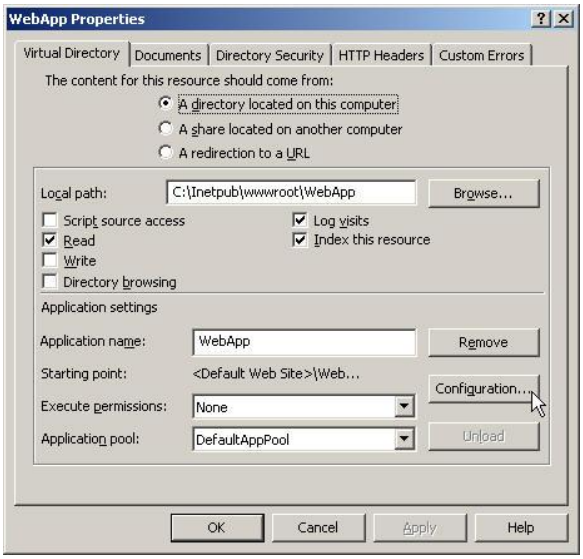
1. In **IIS Manager**, right-click the folder for the Web program that was created, and then click **Properties**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

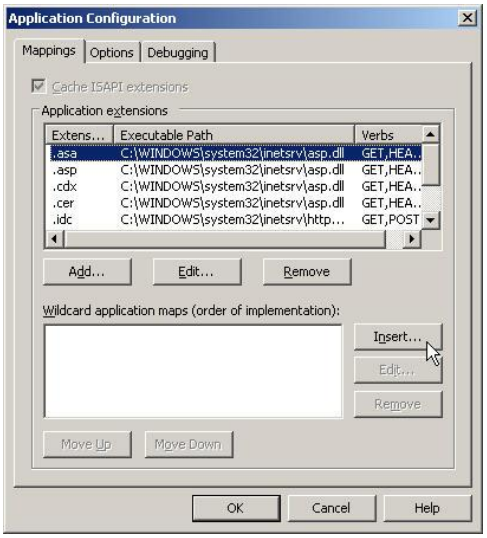


2. In the **Properties** dialog box, click the **Virtual Directory** tab, and then click **Configuration**.

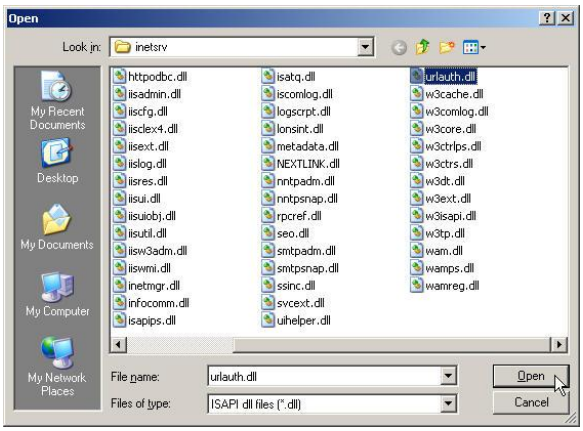


3. In the **Wildcard application maps (order of implementation)** area, click **Insert**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. In the **Add/Edit Application Extension Mapping** dialog box, click **Browse**.
5. Locate the *Systemroot***System32\InetSrv** folder.
6. Select **URLAuth.dll**, and then click **Open.**



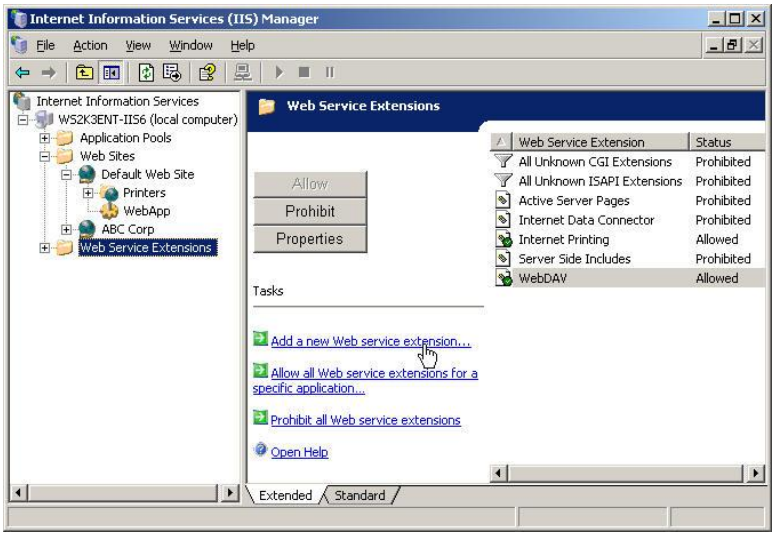
7. Click **OK** three times.

Note: An error message may appear that is similar to "**This executable path is already used**." The appearance of this message means that the URLAuth.dll file is already configured for wildcard program extension mapping.

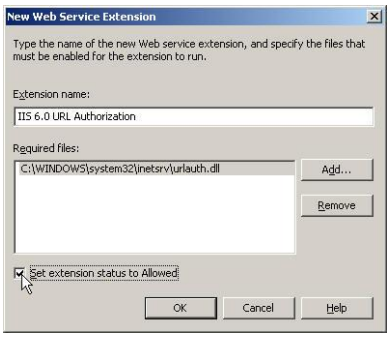
Step 3 - Add the URLAuth.dll file as a new Web service extension

1. In **IIS Manager**, expand **Internet Information Services**, expand the name of the computer that is running IIS, and then select **Web Service Extensions**.
2. In the **Task** list in the details pane, click **Add a new Web service extension**.

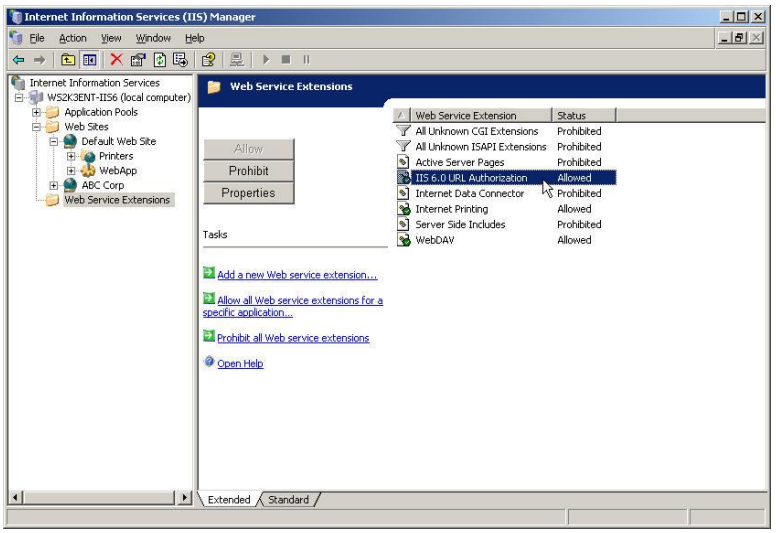
Copyright © 2008 Microsoft Corporation.
All rights reserved.



3. Click **Add**, and then click **Browse**.
4. Locate *Systemroot\System32\InetSrv*, select **URLAuth.dll**, click **Open**, and then click **OK**.
5. In the **Extension Name** box, type **IIS 6.0 URL Authorization**. The exact name, **IIS 6.0 URL Authorization**, must be used.
6. Click to select the **Set extension status to Allowed** check box, and then click **OK**.



7. The **IIS 6.0 URL Authorization** Web service extension will appear in the details pane.

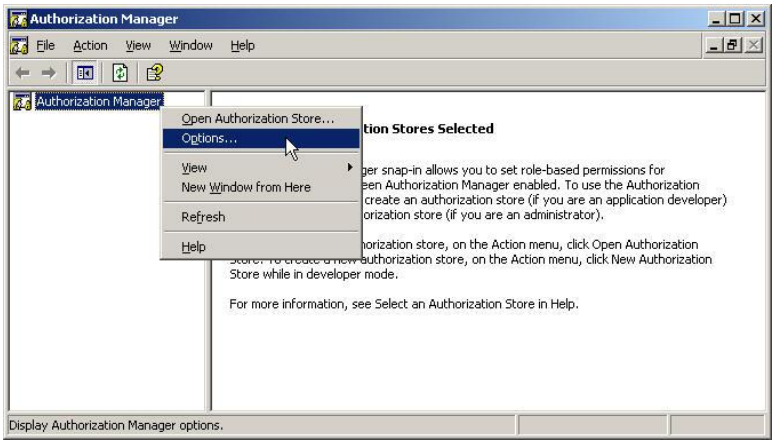


Copyright © 2008 Microsoft Corporation.
All rights reserved.

Step 4 – Create an Authorization Policy

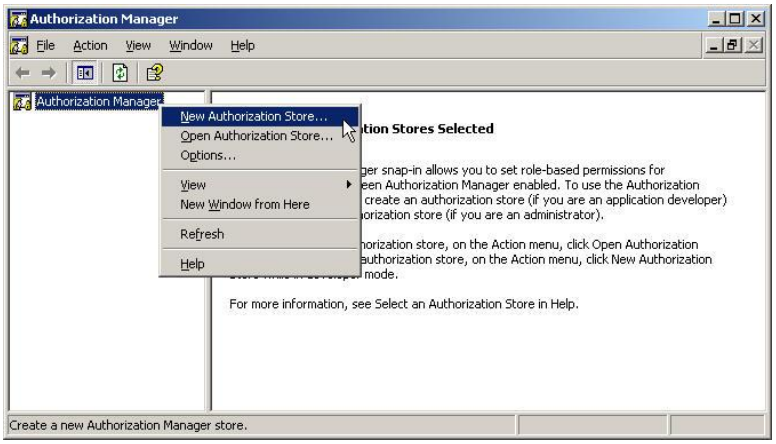
In this example, the Authorization Manager is used to create an authorization policy store that is named MyStore.xml, which is then placed in the **C:\AuthPolicy** folder.

1. Create a folder for the authorization store. For example; **C:\AuthPolicy**.
2. Click **Start**, click **Run**, type **Azman.msc**, and then click **OK**.
3. In the console tree, right-click **Authorization Manager**, and then click **Options**.



4. Click **Developer mode**, and then click **OK**.

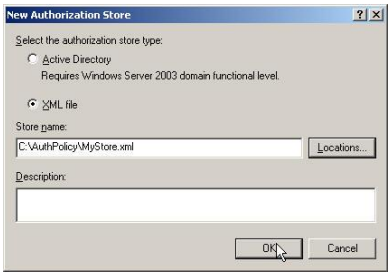
5. In the console tree, right-click **Authorization Manager**, and then click **New Authorization Store**.



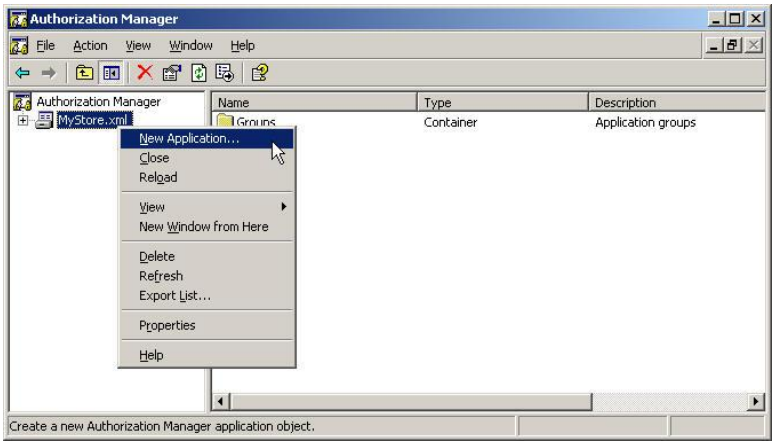
6. Click **XML file**, and then type **C:\AuthPolicy\MyStore.xml** in the **Store name** box. In the **Description** box, information about the new store may be entered. This step is optional. Click **OK**.

Copyright © 2008 Microsoft Corporation.

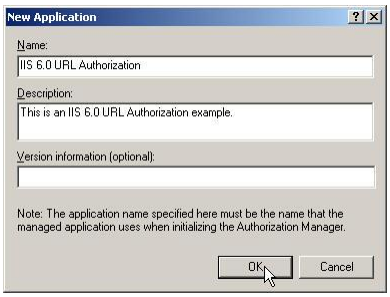
All rights reserved.



7. In the console tree, right-click **MyStore.xml**, and then click **New Application**.

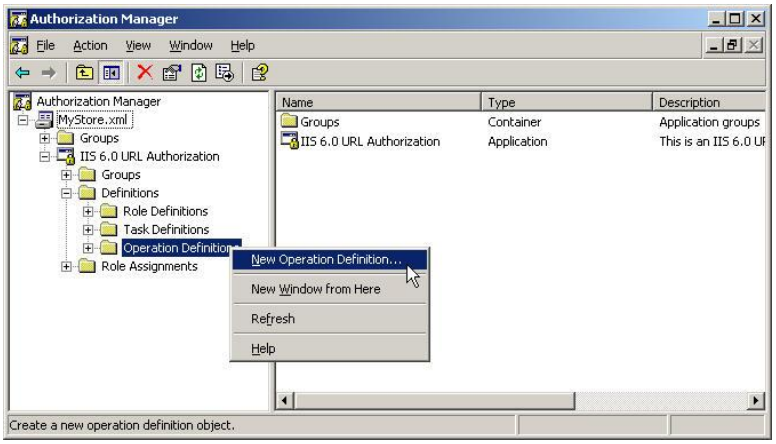


8. In the **Name** box, type **IIS 6.0 URL Authorization**. In the **Description** box, type any information about this usage of ***IIS 6.0 URL Authorization***. This step is optional. Click **OK**.



9. In the console tree, expand **Authorization Manager**, expand **MyStore.xml**, expand **IIS 6.0 URL Authorization**, and then expand **Definitions**.

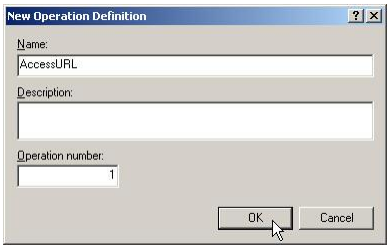
10. Right-click **Operation Definitions**, and then click **New Operation Definition**.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

11. In the **Name** box, type **AccessURL**.
12. In the **Operation number** box, type **1**, and then click **OK**.

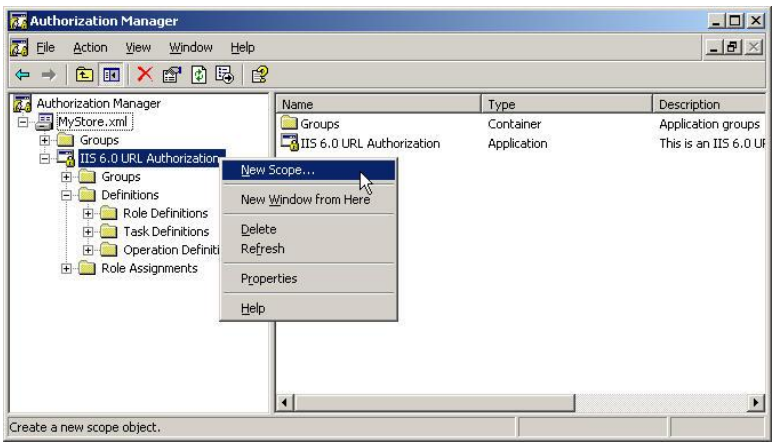


13. In Windows Explorer, go to the authorization policy store location. In the example above, it is **C:\AuthPolicy\MyStore.xml**. Right-click on the authorization policy file, select **Properties**, and then select the **Security** tab. Add the appropriate permissions for authorized users of the store. For this example, Read and Execute permissions are sufficient.

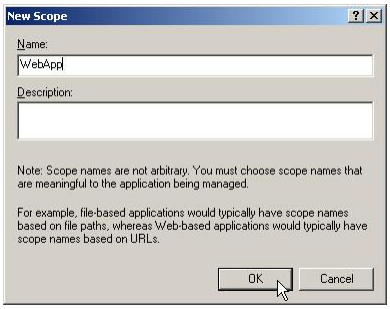
Note: The authorized users will be given the Viewer role in Step 5 as described below.

Step 5 - Set up the scope for the program

1. In the **Authorization Manager** console tree, right-click **IIS 6.0 URL Authorization**, and then select **New Scope**.



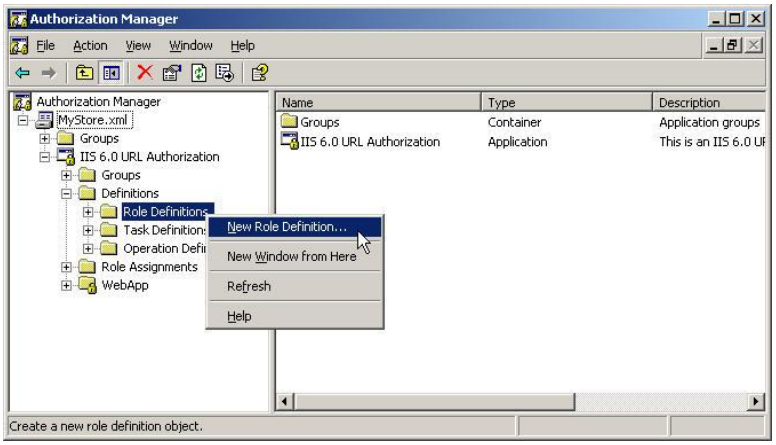
2. In the **Name** box, type **WebApp**, and then click **OK**.



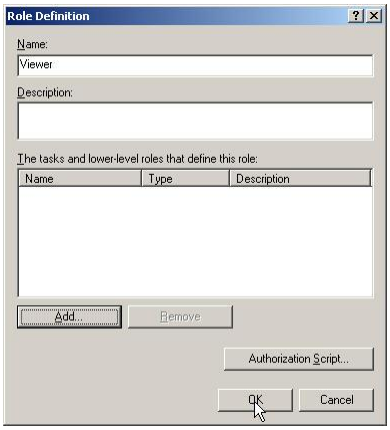
3. In the console tree, expand **IIS 6.0 URL Authorization**, expand **Definitions**, right-click **Role Definitions**, and then select **New Role Definition**.

Note: This role definition can also be created in the **WebApp** scope.

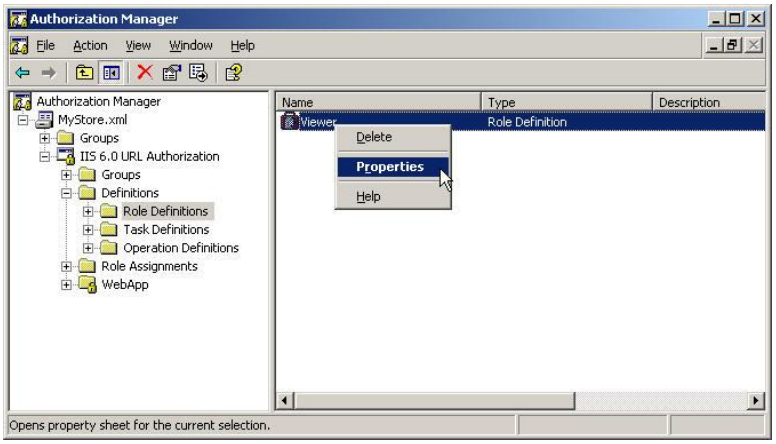
Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. In the **Name** box, type **Viewer**, and then click **OK**.

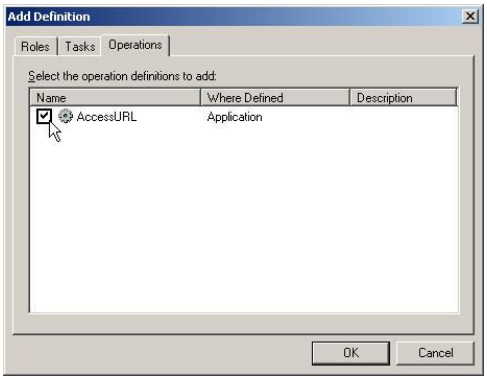


5. In the console tree, select **Role Definitions**.
6. In the details pane, right-click **Viewer**, and then select **Properties**.

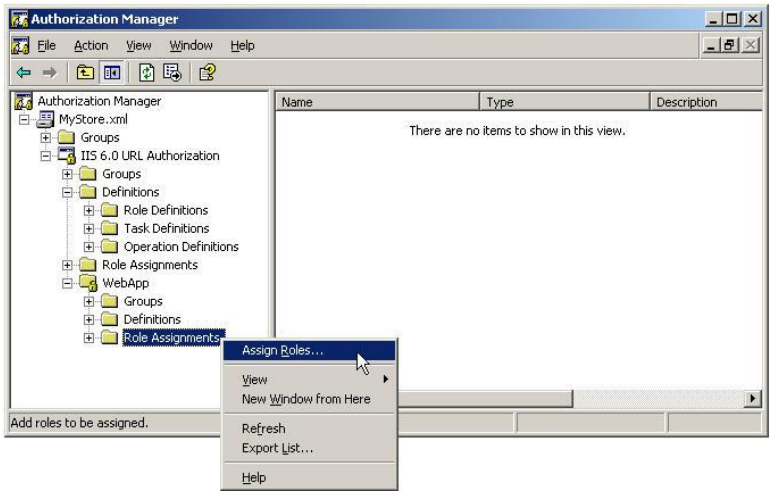


7. Click the **Definition** tab, click **Add**, and then click the **Operations** tab.
8. Click to select the **AccessURL** check box, click **OK**, and then click **OK** again.

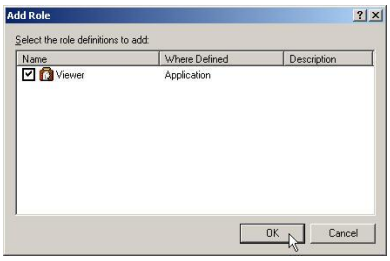
Copyright © 2008 Microsoft Corporation.
All rights reserved.



9. In the console tree, expand **WebApp**, select and right-click **Role Assignments**, and then select **Assign Roles**.

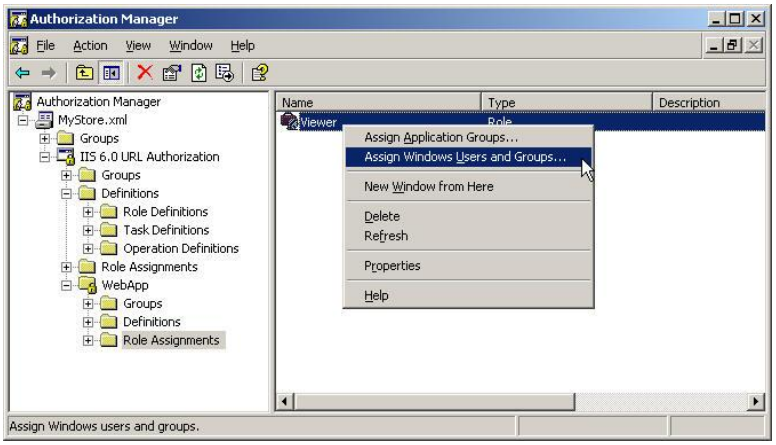


10. Click to select the **Viewer** check box, and then click **OK**.



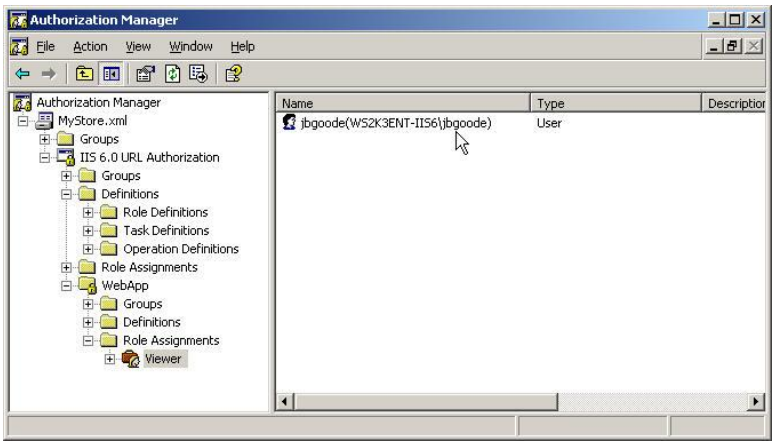
11. In the details pane, right-click **Viewer**, and then select **Assign Windows Users and Groups**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



12. In the **Enter the object names to select (examples)** box, type a user name, and then click **OK**. Click **Check Names** if needed.

13. Double-click **Viewer** to verify the user has been assigned the viewer role.



Step 6 - Add the IIS worker process to the store's Readers role

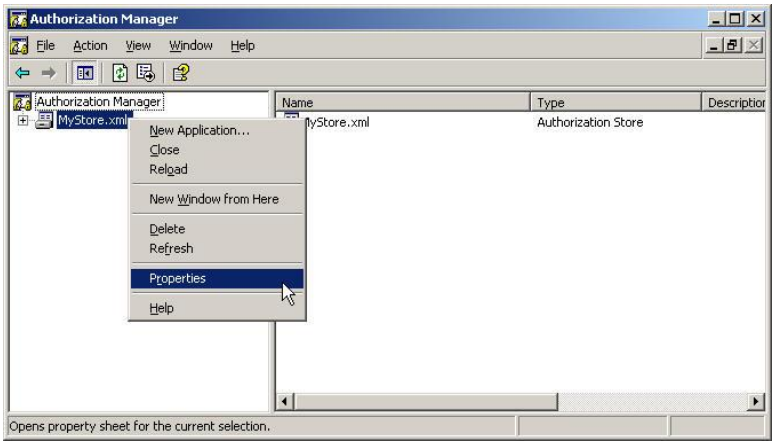
By default, IIS runs under the Network Service account. This example adds Network Service to the Readers role.

> **Note:** If a remote authorization store such as Active Directory or a remote XML file-based store is used, and IIS is running in the default Network Service context, the Active Directory account of the Web server that is running IIS will need to be added to the store's Readers role.

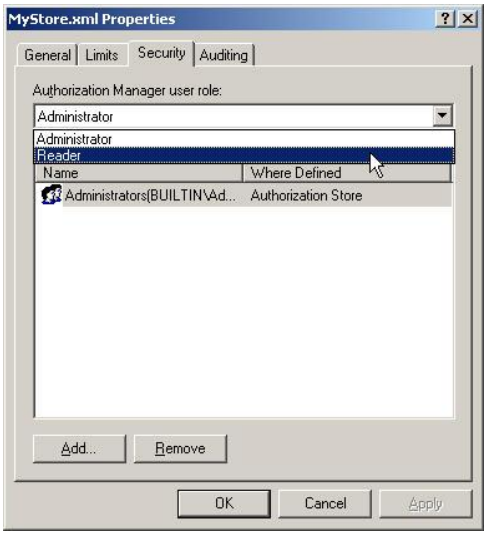
1. In the console tree, right-click the name of the store, and then select **Properties**.

Copyright © 2008 Microsoft Corporation.

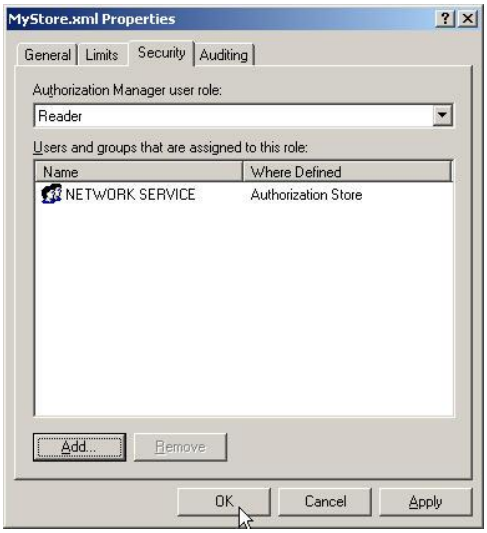
All rights reserved.



2. Click the **Security** tab, click **Reader** in the **Authorization manager user role** list, and then click **Add**.



3. In the **Enter the object names to select (examples)** box, type **Network Service**, click **OK**, and then click **OK** again.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

Step 7 - Configure the IIS metabase to use IIS 6.0 URL Authorization for the Web program

1. Use the script in the "**Sample Script**" subsection to create the SetUrlAuth.vbs file. Save the script file to the **\InetPub\AdminScripts** directory. By default, the **InetPub** directory is in the root of the drive where IIS is installed.
2. Click **Start**, click **Run**, type **Cmd**, and then click **OK**.
3. Change directory to the **\InetPub\AdminScripts** directory.
4. Type the following command, and then press ENTER:

CScript SetUrlAuth.vbs Path of virtual directory AzScopeName value AzStoreName AzEnable value [ImpersonationLevel value]

5. For this example, type the following exactly as shown:

Cscript SetUrlAuth.vbs W3svc\1\Root\WebApp WebApp msxml://C:\AuthPolicy\MyStore.xml true 1

IIS 6.0 URL Authorization is now configured and running for the specified Web program. Users who are in the Viewer role can locate the pages in the program.

Note: If an .xml file is used, append msxml:// to the command as shown in the example above. If the Active Directory Authorization Manager store is used, append msldap:// to the command.

ASP.NET 2.0 Framework Support Service

Administrators can use the ASP.NET 2.0 Microsoft Management Console (MMC) snap-in to configure ASP.NET and ASP.NET applications. The snap-in enables administrators to manipulate ASP.NET 2.0 configuration settings at all levels on local or remote Web servers and the applications they host. The ASP.NET 2.0 MMC snap-in uses the ASP.NET configuration API, but it simplifies the process of editing configuration settings by providing a graphical user interface (GUI). In addition, the tool supports the ASP.NET configuration API features that control whether settings can be inherited by Web applications and are used to manage the dependencies between levels of the configuration hierarchy. The ASP.NET 2.0 MMC snap-in is displayed as an ASP.NET tab on the property sheet of a virtual directory. It includes several interfaces that let administrators manage specific features, such as custom error handling or user authentication.

Configuration Files

ASP.NET configuration data is stored in XML text files named Web.config. Web.config files can appear in multiple directories in within ASP.NET applications. These files allow administrators to easily edit configuration data before, during, or after applications are deployed on the server. Administrators can create and edit ASP.NET configuration files by using the ASP.NET 2.0 MMC snap-in.

Each Web.config file applies configuration settings to the directory that it is in and to all of the child directories below it. Settings applied directly in child directories will override settings that are specified in parent directories. Configuration settings in a Web.config file can optionally be applied to individual files or subdirectories by specifying a path in a location element.

The root of the ASP.NET configuration hierarchy is the `systemroot\Microsoft.NET\Framework\versionNumber\CONFIG\Web.config` file, which includes settings that apply to all ASP.NET applications that run a specific version of the .NET Framework. Because each ASP.NET application inherits default configuration settings from the root Web.config file, administrators need to create Web.config files only for settings that override the default settings.

Copyright © 2008 Microsoft Corporation.

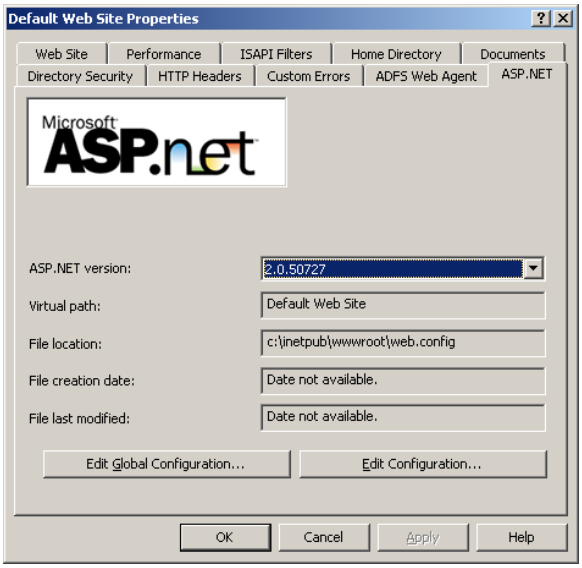
All rights reserved.

Note: The root Web.config file inherits some basic configuration settings from the Machine.config file, which is located in the same directory. Some of these settings cannot be overridden in Web.config files.

At run time, ASP.NET uses the Web.config files to hierarchically compute a unique collection of configuration settings for each incoming URL request. These settings are calculated only once and then cached on the server. ASP.NET detects any changes to the configuration files and then automatically applies those changes to the affected applications, restarting the applications in most cases. Hierarchical configuration settings are automatically calculated and cached again whenever a configuration file in the hierarchy is changed.

Accessing the ASP.NET 2.0 MMC Snap-in

1. Log on as an authorized Web site administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. Under Internet Information Services, expand Servername (local computer), expand Web Sites, right-click either the Web site name or **Default Website**, and then select **Properties**. The Web Site Properties interface is displayed.



4. Click the **ASP.NET** tab, and then click the **Edit Configuration** or the **Edit Global Configuration** button. The ASP.NET Configuration Settings interface is displayed. The Configuration Settings interfaces for the **Edit Configuration** and **Edit Global Configuration** are identical. The difference is that changes made via the **Edit Configuration** interfaces affect the current Web site, whereas changes made via the **Edit Global Configuration** interfaces affect all Web sites hosted by IIS.

Note: Configuration settings can be inherited. Settings can be defined in the Machine.config file, which acts as the base configuration for all Web sites and applications that are on the server. Administrators can create new settings or override inherited settings by making configuration settings at the Web application level, in the Web.config file.

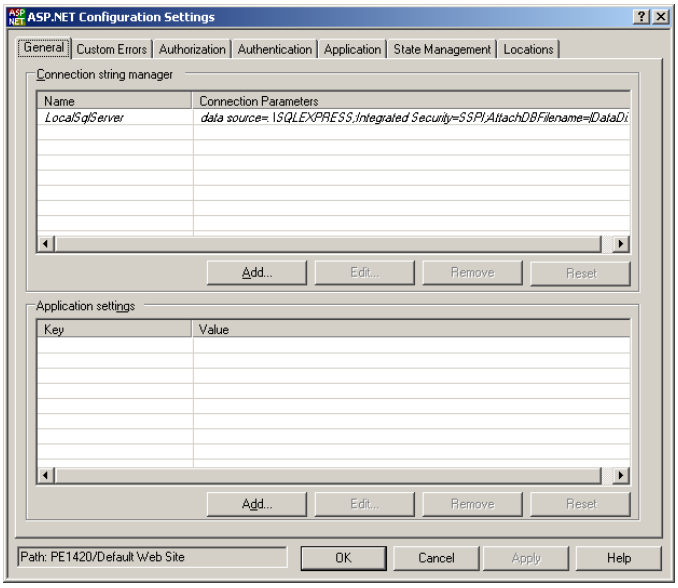
Copyright © 2008 Microsoft Corporation.

All rights reserved.

ASP.NET Configuration Settings – General Tab

The General tab of the ASP.NET Configuration Settings interface enables administrators to manage the following two types of configuration settings:

- **Connection strings**. These settings define information that is used to establish a connection to a data store, such as a database.
- **Application settings**. These settings are simple name/value pairs that let administrators create application-wide values in a central location. Administrators can then access the application values from anywhere within the Web application. By keeping application settings as part of the configuration, administrators can easily change the settings. Application settings are always stored as strings.



The following table explains the elements found on the General tab.

ASP.NET General Tab Configuration Settings	
Element	**Description**
Connection string manager	Lists the connection strings that are defined for the selected Web application. Inherited settings are italic and inherited settings that have been overridden are bold.
Add	Click to display the Edit/Add Connection String interface, where a new connection string can be created.
Edit	Click to display the Edit/Add Connection String interface, where an existing connection string can be edited. Inherited settings can be overridden; in which case, the overridden setting applies only to the selected Web application. Inherited settings cannot be edited to change its value higher in the configuration hierarchy.
Remove	Click to remove or disable the connection string. New settings that are defined for this Web application can be permanently removed. If an inherited setting is removed, the original setting is left intact in its location in the hierarchy and IIS Manager creates a <remove> entry for the setting, which disables the setting.

Copyright © 2008 Microsoft Corporation.

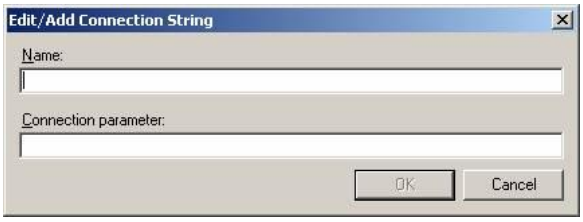
All rights reserved.

ASP.NET General Tab Configuration Settings	
Element	**Description**
Reset	Click to restore an overridden or removed setting to its original value. IIS Manager removes the local, overridden value or deletes the <remove> entry to allow the inherited setting to take precedence.
Application Settings	Lists the application setting key/value pairs.
Add	Click to display the Edit/Add Application Setting interface, where a new key/value pair can be created.
Edit	Click to display the Edit/Add Application Setting interface, where an existing key/value pair can be edited. Inherited settings can be overridden; in which case, the overridden setting applies only to the selected Web application. Inherited settings cannot be edited to change its value higher in the configuration hierarchy.
Remove	Click to remove or disable the key/value pair. New application settings that are defined for this Web application can be permanently removed. If an inherited setting is removed, the original setting is left intact in its location in the hierarchy and IIS Manager creates a <remove> entry for the setting, which disables the setting.
Reset	Click to restore an overridden or removed key/value pair to its original value. IIS Manager removes the local overridden value or deletes the <remove> entry to allow the inherited setting to take precedence.

Edit or add a Connection String property

The Edit/Add Connection String interface allows administrators to create a new ConnectionString property or edit an existing ConnectionString property. The Edit/Add Connection String interface is displayed when the administrator clicks **Add** or **Edit** in the Connection string manager area of the General tab in the ASP.NET Configuration Settings interface. The following procedure explains how to display the Edit/Add Connection String interface from the Microsoft Internet Information Services (IIS) Manager.

1. Open the ASP.NET Configuration Settings interface as described in Accessing the ASP.NET 2.0 MMC Snap-in.
2. Click the **General** tab.
3. Under **Connection string manager**, click **Add** to specify the name for a new ConnectionString property and the Connection parameter or select an existing property and click **Edit** to edit an existing ConnectionString property. The Edit/Add Connection String interface is displayed.



4. Enter the name for the ConnectionString property in the **Name** field. If the Edit/Add Connection String interface is invoked by clicking Edit on the General tab, a name for the connection string cannot be specified.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

5. Enter the value for the ConnectionString property in the **Connection parameter** field. If the Edit/Add Connection String interface is invoked by clicking Edit on the General tab, the Connection parameter box contains the value of an existing ConnectionString property.

Note: Inherited settings can be overridden; in which case, the overridden setting applies only to the selected Web application. Inherited settings cannot be edited to change its value higher up in the configuration hierarchy.

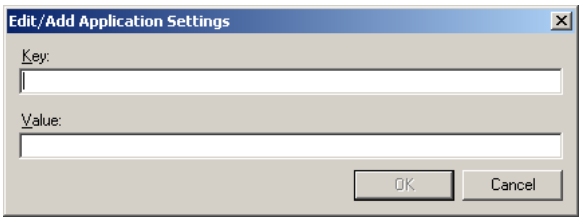
Edit or add application settings

Application settings are simple key/value pairs that let administrators create application-wide values in a central location that can be accessed from anywhere within the Web application. By keeping application settings as part of the configuration in the Web.config file, they can easily be changed. The Application settings dialog box on the General tab displays the list of application setting key/value pairs.

To display the Edit/Add Application Settings dialog box, administrators can click **Add** in the Application settings part of the General tab in the ASP.NET Configuration Settings dialog box. Then, the administrator can specify the key and value for the AppSettings property, which are added to the Application Settings dialog box and the Web.config file for the Web application.

Similarly, administrators can select a setting in the Application settings dialog box, and then click **Edit**. Then, administrators can change the value of the selected AppSettings property. The changes are added to the Application settings dialog box and the Web.config file for the Web application. The following procedure explains how to display the Edit/Add Application Settings dialog box from the Microsoft Internet Information Services (IIS) Manager.

1. Open the ASP.NET Configuration Settings interface as described in Accessing the ASP.NET 2.0 MMC Snap-in.
2. Click the **General** tab.
3. Under **Application Settings**, click **Add** to specify new application settings or select an existing property and click **Edit** to edit existing application settings. The Edit/Add Application Settings interface is displayed.



4. Enter a new key for a key/value pair in the **Key** field. If **Edit** was clicked, a new key in textbox cannot be specified.
5. Enter the value for a key/value pair in the **Value** field. If **Edit** was clicked, the value of the selected key/value pair can be changed.

ASP.NET Configuration Settings – Custom Errors Tab

When an error occurs in an ASP.NET Web page or component, ASP.NET raises an error code. Errors can include the following types:

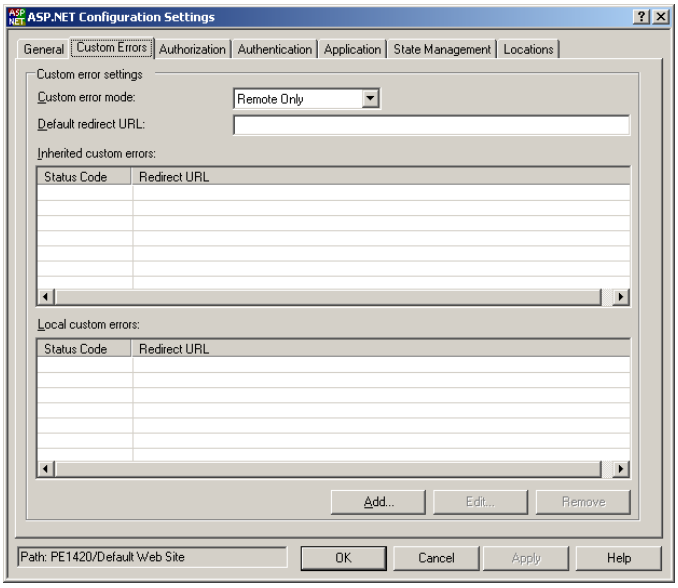
- Compile-time
- Parser (malformed ASP.NET elements)

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Configuration
- Run-time

By default, ASP.NET dynamically generates an error page that contains a description of the error, the name of the page on which the error occurred, and a stack trace. If debug mode is enabled, the dynamically generated page also includes an excerpt of the source code where the error originated. By defining custom errors, administrators can specify how the Web application responds when an error occurs.

Note: For information about debugging mode, see Application Tab, ASP.NET Configuration Settings Interface.



Administrators can use the Custom Errors tab to perform the following tasks:

- Specify a default error page to display when an ASP.NET error occurs anywhere in the Web application.
- Map specific HTTP error codes to corresponding error pages.

Note: Mappings work only for errors that ASP.NET is notified of. For example, by default, ASP.NET is not notified of HTTP 404 errors (page not found). If administrators want ASP.NET to receive these errors, they can set the Web site properties to map HTTP errors to .aspx pages.

- Specify whether custom error pages are displayed for all users, no users, or remote (non-administrative) users.

The following table explains the elements found on the Custom Errors tab.

ASP.NET Custom Errors Tab Configuration Settings	
Element	**Description**
Custom error mode	Click a mode to specify how custom errors are displayed, as follows: ▪ **On**. Custom error pages are always displayed. Use this setting to view errors while developing the Web application. ▪ **Off**. Custom error pages are not displayed. Instead, errors result in a dynamically generated ASP.NET error page.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

ASP.NET Custom Errors Tab Configuration Settings	
Element	**Description**
	▪ **Remote Only**. Errors are redirected only for requests that do not originate locally on the Web server. Use this mode to view ASP.NET errors while working on the server, but display custom errors the Web application users.
Default redirect URL	Type the page name (.aspx or .htm) to display in response to unhandled errors anywhere in the Web application.
Inherited custom errors	Lists the custom error pages that are inherited from configuration files that are higher in the hierarchy. The inherited error settings can be overridden by adding a local custom error for the status code to be overridden.
Local custom errors	Lists the error pages for the current Web site, specifically.
Add	Click to open the Edit/Add Custom Error Handlers interface to specify an HTTP error code and the page to display when ASP.NET detects the error. Note: Mappings work only for errors that ASP.NET is notified of. For example, by default, ASP.NET is not notified of HTTP 404 errors (page not found). For ASP.NET to receive these errors, set the Web site properties to map HTTP errors to .aspx pages. Provide the HTTP error code and the URL of the page it maps to. The page referenced does not have to be in the current Web site. **Note:** IIS Manager does not validate the entered URL.
Edit	Click to open the Edit/Add Custom Error Handlers interface where the page name or error code can be changed for the selected page specified under Local custom errors.
Remove	Click to delete an error page mapping.

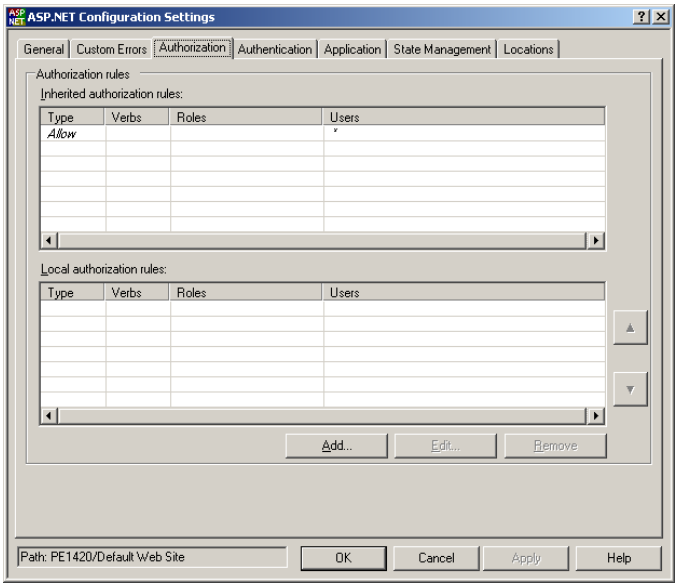
ASP.NET Configuration Settings – Authorization Tab

The Authorization tab of the ASP.NET Configuration Settings interface enables administrators to manage authorization rules for the current Web site directory based on user accounts and roles. Administrators can create user accounts and roles by using Microsoft Windows authentication or ASP.NET Forms authentication (ASP.NET membership). Through the Authorization tab, Web site administrators can view authorization rules that are defined in all inherited configuration files, including the Machine.config file. They can also add, edit, or remove rules for the current Web site directory. Rules are applied to the current subdirectory and all child subdirectories of the current URL unless otherwise overwritten by a configuration file setting in the child subdirectory.

Inherited rules from the Machine.config configuration file and any parent virtual directory also appear, but cannot be edited. To change the effect of inherited rules, administrators can create new settings at the Web site level. Application settings are always stored as strings.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



The following table explains the elements found on the Authorization tab.

ASP.NET Authorization Tab Configuration Settings	
Element	**Description**
Inherited authorization rules	Lists the inherited authorization rules that are defined in the Machine.config file or any parent virtual directory, as defined in ASP.NET Configuration File Hierarchy and Inheritance. Inherited settings are italic and inherited settings that are overridden are bold.
Local authorization rules	Lists the authorization rules that are applied to the current Web site directory and to all its child directories.
Add	Click to open the Edit Rule Interface to create a new rule.
Edit	Click to open the Edit Rule Interface to edit the selected rule.
Remove	Click to delete the selected row from Local authorization rules.

Authorization rules are applied in order, from top to bottom. In some cases, an administrator might have to create multiple rules for the same folder in order to establish the correct permissions. For example, an administrator might create a rule that denies access to anonymous user accounts and a second rule that denies access to user accounts in the role of Guest. That way, only users who are logged on (users who are not anonymous) and in another group (not Guest) can gain access the folder.

The Web.config settings that are managed through the Authorization tab is the `<authorization>`, `<roleManager>` section. The following excerpt from a sample Web.config file restricts access to a subdirectory of the Web site. Access to the restricted subdirectory is allowed for administrators and for the user named John, and is denied for anonymous users.

<?xml version="1.0" encoding="utf-8"?> <configuration> <system.web> <authorization> <allow roles="administrators" /> <allow users="John"/> <deny users="?" /> </authorization> </system.web> </configuration>

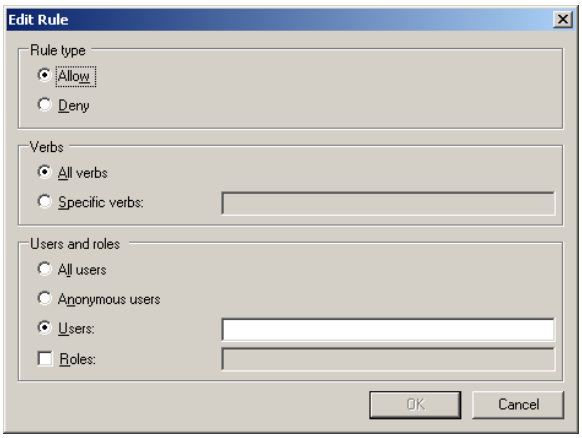
Copyright © 2008 Microsoft Corporation.

All rights reserved.

Create or edit an authorization rule

The Edit Rule interface enables administrators to create a new authorization rule or edit an existing one. User accounts and roles are created using Microsoft Windows authentication or ASP.NET Forms authentication (ASP.NET membership). The following procedure explains how to open the Edit Rule interface.

1. Open the ASP.NET Configuration Settings interface as described in Accessing the ASP.NET 2.0 MMC Snap-in.
2. Click the **Authorization** tab.
3. To add a rule, click **Add** or to edit a rule, select a rule, and then click **Edit**. The Edit Rule interface is displayed.



4. The following table explains the options that can be selected on the Edit Rule interface.

Authorization Rule Configuration Settings	
Element	**Description**
Rule type	Click Allow to allow all users access. Click Deny to deny all users access.
Verbs	Click All Verbs to specify that all ASP.NET HTTP transmission methods are allowed access. All Verbs is the default. To limit authorization to specific HTTP verbs, click Specific verbs, and then type a comma-separated list of the HTTP transmission methods that are granted access. Verbs that are registered to ASP.NET are GET, HEAD, POST, and DEBUG.
Users and roles **Note: This setting is required.**	Complete one or more of the following actions to apply the rule: To apply the rule to all users, click All users. To apply the rule to only to users who are not logged in, click Anonymous users. To apply the rule to a specific set of user accounts, click Users, and then type a comma-separated list of user account names. To apply the rule to a specific set of roles, select the Roles check box, and then type a comma-separated list of role names. If both Users and Roles is specified, the rule applies only to user accounts that are in the specified roles. Use Windows authentication or ASP.NET Forms authentication (ASP.NET membership) to define user accounts and roles.

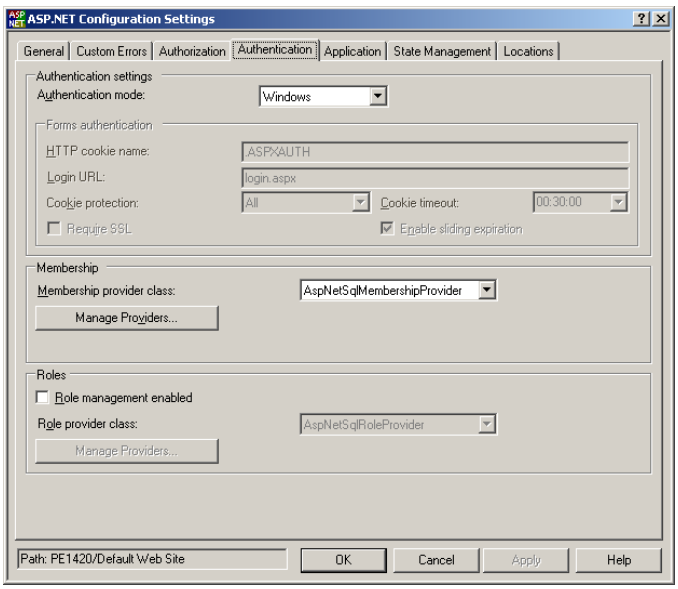
Copyright © 2008 Microsoft Corporation.
All rights reserved.

5. Once the desired authorization rule settings have been selected, click **OK** to accept the settings.

ASP.NET Configuration Settings – Authentication Tab

The Authentication tab of the ASP.NET Configuration Settings interface enables administrators to manage authentication of user accounts and roles for the current Web site. ASP.NET Authentication is the process of obtaining identification credentials, such as a user name and password from a user account, for validating the credentials against some authority.

The Authentication tab also provides support to add, remove, and configure membership providers and role management for the current Web application. ASP.NET role management lets administrators specify the resources that user accounts can access in the application. Role management lets administrators treat groups of user accounts as a unit by assigning user accounts to roles.



The following table explains the elements found on the Authentication tab.

ASP.NET Authentication Tab Configuration Settings	
Element	**Description**
Authentication mode	Click to specify the authentication mode for the current Web site.
HTTP cookie name	Type the name of the HTTP cookie to use for authentication in the current Web site. **HTTP cookie name** is only available for configuring Forms authentication.
Login URL	Type the URL to which the request is redirected for log on, if no valid authentication cookie is found. The default is login.aspx. **Login URL** is only available for configuring Forms authentication.
Cookie protection	Click to specify the type of encryption, if any, to use for the authentication cookie. **Cookie protection** is only available for configuring Forms authentication.
Cookie timeout	Enter the amount of time, in integer minutes, after which the authentication cookie expires. The default is 30. **Cookie timeout** is only available for configuring Forms authentication.
Require SSL	Select this check box to specify that an SSL connection is required to transmit the authentication cookie. **Require SSL** is only available for configuring Forms authentication.

Copyright © 2008 Microsoft Corporation.

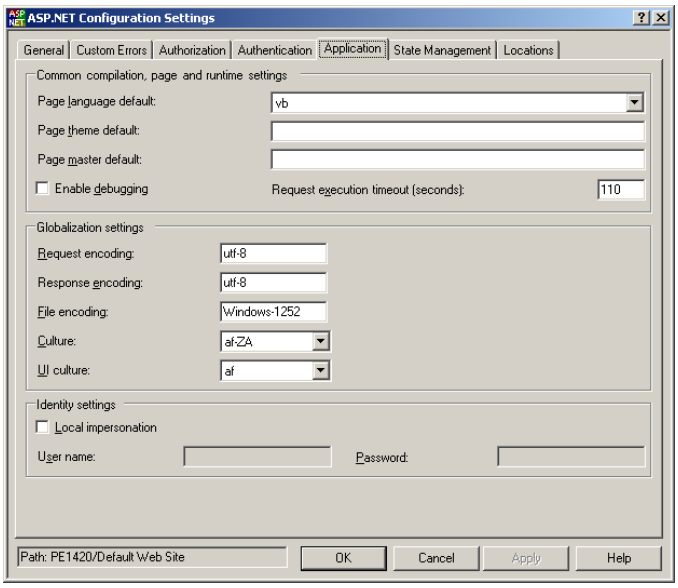
All rights reserved.

ASP.NET Authentication Tab Configuration Settings	
Element	**Description**
Enable sliding expiration	Select this check box to reset the expiration time for a valid authentication cookie, if a request is made and more than half of the timeout interval has elapsed. **Enable sliding expiration** is only available for configuring Forms authentication.
Membership provider class	Click to specify the configured membership providers for the current Web site.
Membership: Manage Providers	Click to open the Provider Settings interface to add, remove, and configure membership providers for the current Web site.
Role management enabled	Select this check box to enable role management to manage access rules for groups of user accounts.
Role provider class	Click to specify the configured role membership providers for the current Web site.
Roles: Manage Providers	Click to open the Provider Settings interface to add, remove, and configure role membership providers for the current Web site.

ASP.NET Configuration Settings – Application Tab

The Application tab of the ASP.NET Configuration Settings interface enables administrators to manage three types of configuration settings:

- Common compilation, page, and run-time settings
- Globalization settings
- Identity settings



Administrators can use the Application tab to perform the following tasks:

- Set the default language for the ASP.NET pages in the Web application.
- Set the default theme and master page for the Web application.
- Enable debugging for the Web application.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Specify the maximum number of seconds a request can run before it is automatically shut down by ASP.NET.
- Set content encoding character sets for requests, responses, and culture settings, which determine the results of culture-dependent functions, such as the date, number, and currency formatting.
- Set the Windows identity that will be impersonated and under which the ASP.NET pages run.

The following table explains the elements found on the Application tab.

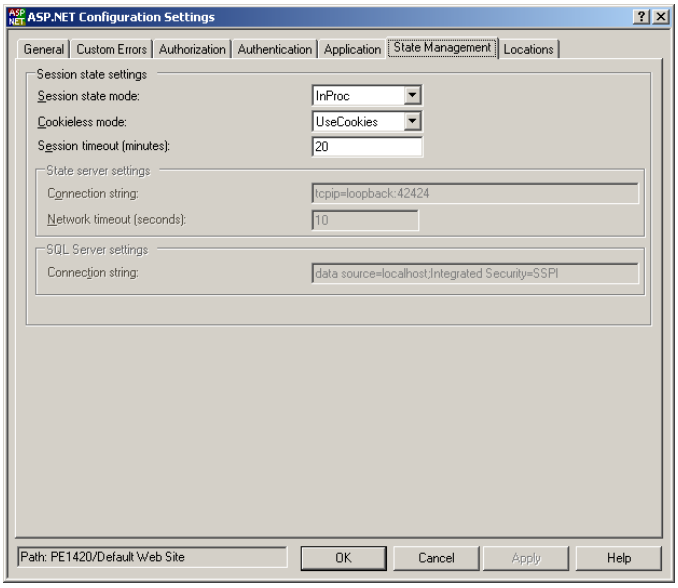
ASP.NET Application Tab Configuration Settings	
Element	**Description**
Common Compilation, Page and Runtime Settings	Lets administrators make configuration settings for Page Language Default, Page Theme Default, Page Master Default, Enable Debugging, and Request Execution Timeout (seconds).
Page Language Default	Lets administrators select the default programming language to use in dynamic compilation files. The available languages are VB (Microsoft Visual Basic development system), C#, JS (Microsoft JScript development software), and VJ# (Microsoft Visual J# development tool).
Page Theme Default	Lets administrators specify the default theme to apply to all pages in the Web application.
Page Master Default	Lets administrators specify the path for the master page file relative to the local configuration file.
Enable Debugging	Lets administrators specify whether to compile retail or debug binaries. The value is false, if the check box is clear.
Request Execution Timeout (seconds)	Lets administrators set the maximum number of seconds that a request is allowed to execute before being automatically shut down by ASP.NET.
Globalization Settings	Lets administrators make configuration settings for Request Encoding, Response Encoding, Culture, and UI Culture.
Request Encoding	Lets administrators specify the assumed encoding of each incoming request, including posted data and the query string. The default is UTF-8.
Response Encoding	Lets administrators specify the content encoding of responses. The default is UTF-8.
File Encoding	Lets administrators specify the default encoding for .aspx, .asmx, and .asax file parsing.
Culture	Lets administrators select the default culture for processing incoming Web requests. The culture determines the results of culture-dependent functions, such as the date, number, and currency formatting.
UI Culture	Lets administrators select the default culture for processing incoming Web requests. The culture determines the results of culture-dependent functions, such as the date, number, and currency formatting.
Identity Settings	Lets administrators make configuration settings for Impersonate, User Name, and Password.
Impersonate	Lets administrators specify whether client impersonation is used on each request.
User Name	Lets administrators specify the user name to use, if client impersonation is used on each request.
Password	Lets administrators specify the password to use, if client impersonation is used on each request.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

ASP.NET Configuration Settings – State Management Tab

The State Management tab of the ASP.NET Configuration Settings interface lets administrators manage state and page information over multiple requests for the pages in the current Web site. ASP.NET session state lets administrators store and retrieve values for a user account as the user navigates the different ASP.NET pages that make up a Web application. The State Management tab lets the administrator configure how and where the values are stored.



Using the State Management tab, an administrator can do the following:

- Select the session-state mode for the current Web application.
- Configure the **SQLServer** and **StateServer** session-state modes.

The following table explains the elements found on the State Management tab.

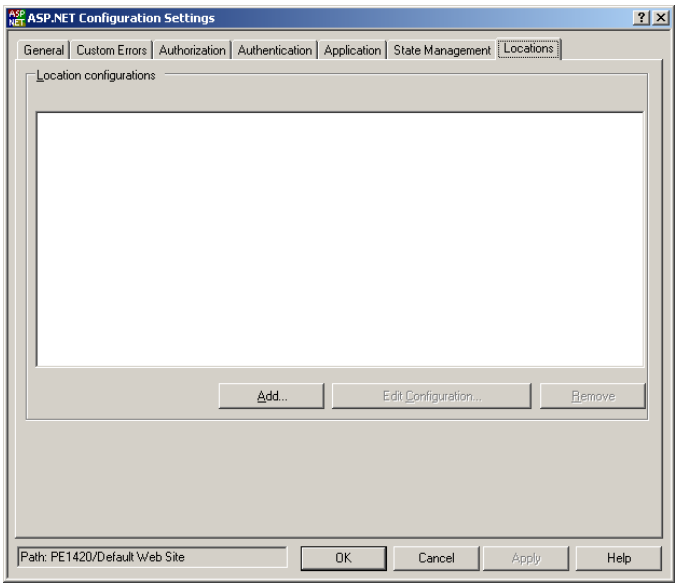
ASP.NET State Management Tab Configuration Settings	
Element	**Description**
Session state mode	Click a session-state mode. The default session-state mode is InProc, or in memory on the Web server.
Cookieless mode	Click a cookie mode to define when to use a cookie to maintain information about the user.
Session Timeout	Enter the time, in minutes, that is allowed between requests before the session is terminated.
Connection string	Enter the connection string to identify the server name and port for the ASP.NET state service for the StateServer mode.
Network timeout	Enter the time, in seconds, that is allowed between requests before the network session is terminated for the StateServer mode.
Connection string	Enter the connection string to identify the server name and port for the SQLServer mode.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

ASP.NET Configuration Settings – Locations Tab

Configuration settings can be applied to a specific Web application or directory by using a location tag with an appropriate path attribute. The path attribute can be used to identify a specific file or child directory to which unique configuration settings apply. Using the Locations tab of the ASP.NET Configuration Settings interface is a way to embed configuration settings inside a configuration file.

Administrators can use the Locations tab to specify the path location configurations that are defined in the configuration file for a node.



The following table explains the elements found on the Locations tab.

ASP.NET Locations Tab Configuration Settings	
Element	**Description**
Location configurations	Displays the path location configurations that are defined in the configuration file for a node.
Add	Lets administrators display the Add Location interface to specify an index and a location to add a new location to the Location Configuration interface in the ASP.Net configuration Settings interface.
Edit Configuration	Lets administrators display a new ASP.NET Configuration Settings tab for the node that is specified by the path in the containing configuration file.
Remove	Lets administrators remove a location entry from the configuration file for this node.

Add a new location configuration setting

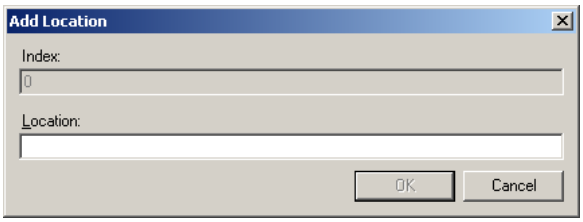
The Add Location interface enables administrators to add a new location configuration setting to a Web site. Configuration settings can be applied to specific resources by using a `<location>` tag with an appropriate path attribute. The path attribute can be used to identify a specific file or child directory to which unique configuration settings apply. The following procedure explains how to display the Add Location interface from IIS Manager.

1. Open the ASP.NET Configuration Settings interface as described in Accessing the ASP.NET 2.0 MMC Snap-in.
2. Click the **Locations** tab.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. Click **Add**. The Add Location interface is displayed.



4. Specify the value of the item being added to list in the **Location** field. (For example, the path to a specific file or directory).
5. Click **OK** to apply the location value.

Background Intelligent Transfer Service

The Background Intelligent Transfer Service (BITS) is a background file transfer mechanism and queue manager used to assist with the transfer of large amounts of data without degrading network performance. BITS throttles file requests to minimize bandwidth consumption by transferring data in small chunks, utilizing unused bandwidth as it becomes available, and reassembling the data at the destination. Any transfers that are interrupted by network disconnections or by computer shutdowns and restarts are resumed when network connectivity is re-established.

Requests to BITS are submitted by an application, such as Automatic Updates, and the files can be transferred in a throttled manner such that the interactive user is not affected by the bandwidth consumed. Requests are placed in a queue until the files are transferred, at which time the requesting application is invoked and notified of the completion.

BITS Server Extensions

Enable BITS Server Extensions with IIS in order to maintain Web server quality of service. BITS Server Extensions has the following components:

- **BITS Server Extensions ISAPI**: Enable this option to throttle IIS requests with the help of the BITS server.
- **BITS Server Extensions Snap-in**: Install this snap-in to access and view the BITS graphical user interface (GUI) used to configure and managing BITS on the local Web server.

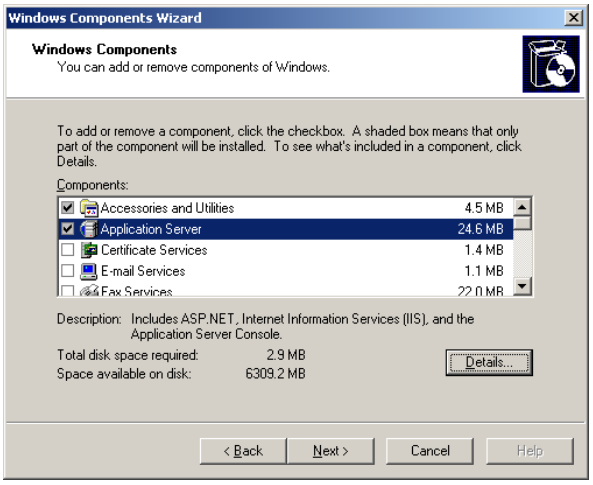
If it is desired that client computers be able to use BITS to upload files to a server, an IIS server must be configured with BITS Server Extensions installed and activated.

BITS Server Extensions Installation

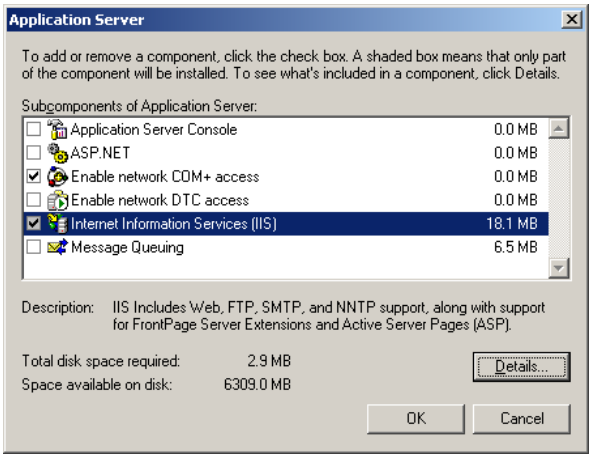
To install BITS Server Extensions support on an IIS server, follow the steps below.

1. Log on as an authorized administrator.
2. Click **Start** and then select **Control Panel.**
3. Double-click **Add or Remove programs** and then click **Add or Remove Windows Components**. The Windows Component Wizard is displayed.

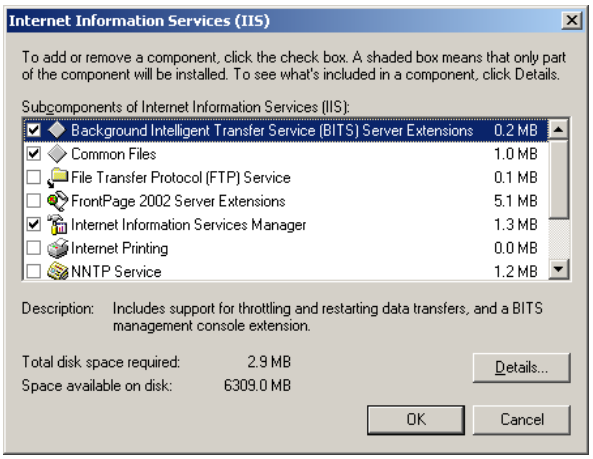
Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. From the Windows Components Wizard, select **Application Server**, and then click **Details**. The Application server interface is displayed.



5. In the Application Server interface, select **Internet Information Services (IIS)**, and then click **Details**. The Internet Information Services (IIS) interface is displayed.

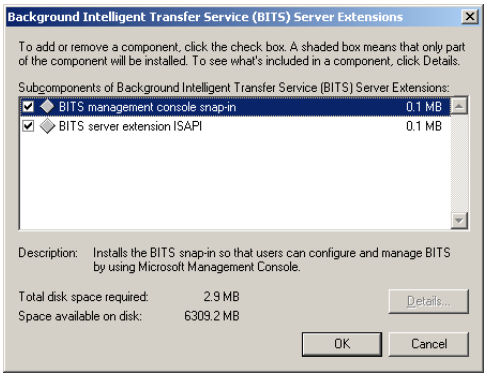


6. In the Internet Information Services (IIS) interface, check **Background Intelligent Transfer Service (BITS) Server Extensions,** and then click **Details**. The Background Intelligent Transfer Service (BITS) Server Extensions interface is displayed. By default, both the BITS server extension ISAPI and the BITS management console snap-in are installed. To view each selection individually, click **Details**

Copyright © 2008 Microsoft Corporation.

All rights reserved.

in the Internet Information Services (IIS) interface to open the Background Intelligent Transfer Service (BITS) server extension interface.



7. Close the Intelligent Transfer Service (BITS) server extension, Internet Information Services (IIS), and the Application Server interfaces by clicking **OK** on each one to return to the Windows Component Wizard. Then click **Next** to begin the installation of BITS Server Extensions as part of Application Server. The wizard completes the installation.

Notes: To install BITS Server Extensions, files from the Windows Server 2003 installation media may be required. Ensure that the media is available.

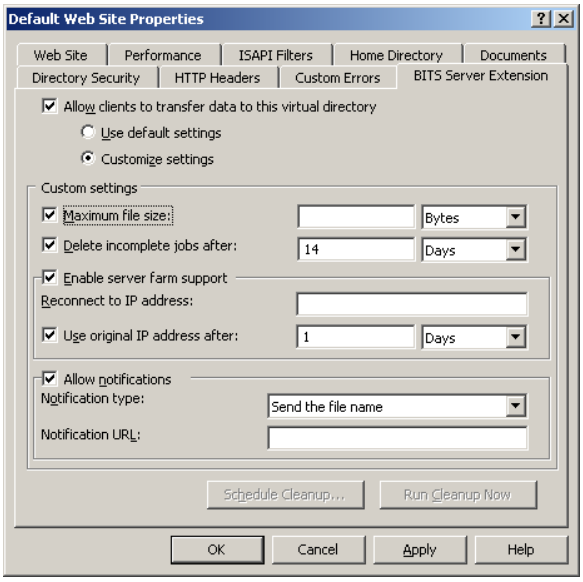
BITS Server Extensions Configuration

Configuring BITS Server Extensions requires the use of Internet Information Services (IIS) Manager. Follow the procedures below to start Internet Information Services (IIS) Manager so that BITS Server Extensions settings may be viewed and configured.

1. Log on as an authorized administrator.
2. Click **Start**, point to **Administrative Tools**, and then select **Internet Information Services (IIS) Manager**.
3. Expand the nodes under the server where BITS Server Extensions is installed, and then expand the Web Sites folder.
4. Right-click the desired virtual directory for BITS Server Extensions configuration and then select **Properties**.
5. In the Properties interface, select the **BITS Server Extensions** tab to display its configuration settings.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



BITS Server Extensions Configuration Settings

The BITS Server Extensions Configuration tab is grouped in the following sections.

Note: Configuration settings can be inherited. If the directory is a subdirectory of another virtual directory and the parent virtual directory defines a custom configuration, the configuration of the parent virtual directory is used instead of the default settings.

BITS Server Extensions Settings	
Configuration group	**Description**
Allow clients to transfer data to this virtual directory	Enables uploads from BITS clients into the virtual directory. If this check box is not checked, BITS clients attempting an upload are denied access. ▪ **Use default settings**. Precludes configuring BITS Server Extensions for the virtual directory. The remaining settings cannot be configured unless the **Customize settings** radio button is selected. ▪ **Customize settings**. Allows the configuration of this property page according to the settings specified in **Custom settings**.
Custom settings	Permits selection of maximum file size and allows the specification of a time limit after which incomplete jobs can be deleted. ▪ **Maximum file size**. Defines the maximum size of a file that can be uploaded in a single BITS job. If this setting is not enabled, clients can upload files of any size. ▪ **Delete incomplete jobs after**. If enabled permits incomplete upload files to be deleted by the cleanup process if no progress has been made within the specified time period. Deletions are performed only when the cleanup process is scheduled, or when a manual cleanup is run.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

BITS Server Extensions Settings	
Configuration group	**Description**
Enable server farm support	If enabled, instructs the client to try to reconnect to the server of choice instead of the original upload URL used by the client. Server farms can be configured two ways: by using a shared volume for the upload virtual directory, or by using server local storage for the uploaded files. If local storage is desired, this option enables the client computer to reconnect to the same server computer in the server farm. **Note:** Server farm support is not included in the TOE. ▪ **Reconnect to IP address**. Specifies the public IP address to use for reconnecting to this server. A server usually has two IP addresses. One points outward and is reachable by client systems. The other belongs to the inner (protected) network. Specification of the outward-pointing IP address is completed here. ▪ **Use original IP address after**. Specifies the amount of time during which a client computer must reconnect to the server specified in **Reconnect to IP address**. If the client computer does not connect to the server during this time, the client computer must attempt to connect to the original DNS name specified in the upload URL.
Allow notifications	Enables notifications for this virtual directory. Both Notification type and Notification URL settings are required if this setting is enabled. ▪ **Notification types**. Defines what is sent in the notification. If **Send the file name** is selected, the server passes the path for the completed upload file to the URL specified by the Notification URL setting. The server returns a file to the client computer as a response. If **Send the data** is selected, the server passes the entire upload file to the URL specified by the Notification URL as a POST. The response is sent to the client computer. ▪ **Notification URL**. Specifies the URL to pass the completed upload file to via a POST request if the Notification type is either Send the file contents or Send the file name. The URL can be absolute or self-relative. If the URL is self-relative, the original request URL is used as the base.
Schedule Cleanup	Configures the frequency with which BITS Server Extensions scans the virtual directory for incomplete upload files. If an incomplete file is found, it is checked against the time-out value set in **Delete incomplete jobs after**. If the time-out period has elapsed since progress was made on this file, the upload is cancelled and any partial file contents are deleted. This setting is not affected by IIS property inheritance and applies only to the virtual directory.
Run Cleanup Now	Immediately starts a cleanup by scanning the virtual directory for incomplete upload files. If an incomplete file is found, it is checked against the time-out value set in **Delete incomplete jobs after**. If the time-out period has elapsed since progress was made on this file, the upload is cancelled and any partial file contents are deleted. To remove all incomplete files from this virtual directory, set the time-out value to 0 before running the cleanup.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Notes: After configuration setting changes are made on the **BITS Server Extensions** tab and the changes are applied, a security message will appear indicating that BITS will shut down all Run Script and Execute Permissions for this virtual directory. Acknowledging this prompt, by clicking **OK** permits the **Run Cleanup Now** button to be selected. Additionally, BITS Server Extensions must be in the Allowed state in order to function. To determine this state, expand **Web Service Extension** in the IIS console tree, then located the extension state in the right panel. Select **Allowed** if the extension is in the Prohibited state.

Background Intelligent Transfer Service (BITS) Administration Utility

The BITS Administration Utility is a command-line tool (BITSAdmin.exe) that allows administrators to manage the BITS service. Windows Server Update Services (WSUS) and Automatic Update Service use BITS by default. BITS regulates the transfer rate to minimize impact on user interactivity, such as a job sent to a network printer or Web pages viewed through Internet Explorer.

Installing BITSAdmin.exe

BITSAdmin.exe 2.0 is a support tool included on the Windows installation CD. The Support Tools are not automatically installed when Windows is installed.

- To install the Support Tools on a computer that is running Windows XP Professional, run the Setup.exe file from the \Support\Tools folder on the Windows XP CD.
- To install the Support Tools on a computer that is running Windows Server 2003, execute the suptools.msi installer file from the \Support\Tools folder on the Windows Server 2003 CD.

Using BITSAdmin.exe

To run BITSAdmin.exe, perform the following.

1. Log on as an authorized administrator.
2. Click **Start**, click **Run**, type **cmd**, and press **Enter**.
3. At the command prompt type bitsadmin /? and then press **Enter**. This will display BITSAdmin.exe help information, describing command line parameters as shown in the table below.

BITSAdmin.exe Command Parameters

Parameter	Description
/help| /?	Displays command line usage.
/list[/allusers] [/verbose]	Lists transfer jobs. The /allusers parameter lists jobs for all users on the system. The /verbose parameter provides detailed information about jobs.
/monitor[/allusers] [/refreshSeconds]	Monitors the copy manager. The /allusers parameter monitors the copy manager for all users on the system. The /refresh parameter reacquires copy manager data in the specified time interval in seconds.
/reset	Deletes all jobs in the manager. If executed by an administrator, all jobs are deleted. If executed by a normal user, only the jobs owned by the user are deleted.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

BITSAdmin.exe Command Parameters	
Parameter	**Description**
/create [type]DisplayName	Creates a job and assigns DisplayName to it. The type can be /Download, /Upload, or /Upload-Reply.
/infoJob[/verbose]	Displays information about the specified job. The /verbose parameter provides detailed information about the job.
/addfileJobRemoteURL LocalName	Adds a file to the specified job. RemoteURL specifies the file's source location. LocalName specifies the file's name on the local target computer.
/listfilesJob	Lists the files in the specified job.
/suspendJob	Suspends the specified job. The job will not be scheduled to run again until the /resume parameter is executed.
/resumeJob	Queues the job to the list of jobs enabled for transfer.
/cancelJob	Deletes the specified job.
/completeJob	Completes the job and makes the files available for the destination directory. This is normally executed after the job moves to the transferred state.
/gettypeJob	Retrieves the job type of the specified job.
/getbytestotalJob	Retrieves the size of the specified job.
/getbytestransferredJob	Retrieves the number of bytes transferred for the specified job.
/getfilestotalJob	Retrieves the number of files in the specified job.
/getfilestransferredJob	Retrieves the number of files transferred for the specified job.
/getcreationtimeJob	Retrieves the job creation time for the specified job.
/getmodificationtimeJob	Retrieves the job modification time.
/getcompletiontimeJob	Retrieves the job completion time for the specified job.
/getstateJob	Retrieves the job state for the specified job.
/geterrorJob	Retrieves detailed error information for the specified job
/getownerJob	Retrieves the job owner for the specified job.
/getdisplaynameJob	Retrieves the display name for the specified job.
/setdisplaynameJobDisplayName	Sets the DisplayName for the specified job.
/getdescriptionJob	Retrieves the job description of the specified job.
/setdescriptionJobDescription	Sets the description for the specified job.
/getpriorityJob	Retrieves the priority of the specified job.
/setpriorityJobPriority	Sets the priority for the specified job.
/getnotifyflagsJob	Retrieves the notify flags for the specified job.
/setnotifyflagsJobNotifyFlags	Sets the notify flags for the specified job.
/getnotifyinterfaceJob	Determines if notify interface is registered for the specified job.
/getminretrydelayJob	Retrieves the retry delay, in seconds, for the specified job.
/setminretrydelayJobRetryDelay	Sets the RetryDelay, in seconds, for the specified job.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

BITSAdmin.exe Command Parameters	
Parameter	**Description**
/getnoprogresstimeoutJob	Retrieves the no progress timeout, in seconds.
/setnoprogresstimeoutJobTimeout	Sets the no progress Timeout, in seconds, for the specified job.
/geterrorcountJob	Retrieves an error count for the specified job.
/getproxyusageJob	Retrieves the proxy usage setting for the specified job.
/getproxylistJob	Retrieves the proxy list for the specified job.
/getproxybypasslistJob	Retrieves the proxy bypass list for the specified job.
/setproxysettingsJobuse, List, Bypass	Sets the proxy Settings for the specified job.
/takeownershipJob	Takes ownership of the specified job.
/SetNotifycmdlineJobcommand-line	Sets a command line for job notification.
/GetNotifycmdlineJob	Returns the job's notification command line.
/SetCredentialsJobTargetSchemeUser namePassword	Adds credentials to a job. The Target can be either SERVER or PROXY. The scheme can be BASIC, DIGEST, NTLM, NEGOTIATE, or PASSPORT.
/GetreplyfilenameJob	Gets the path of the file containing the server reply.
/SetreplyfilenameJob	Path Sets the path of the file containing the server reply.
/GetReplyProgressJob	Returns the size and progress of the server reply.
/GetReplyDataJob	Retrieves the server's reply data in hexadecimal format.
/rawreturn	Returns data suitable for parsing. Strips new line characters and formatting from the output. This parameter can be used in conjunction with the /create and /get* parameters.
/wrap	Wraps output to fit in a command window.
/nowrapJob	Does not wrap output to fit in a command window.
/RemoveCredentialsJobTargetScheme	Removes credentials from a job. The Target can be either SERVER or PROXY. The scheme can be BASIC, DIGEST, NTLM, NEGOTIATE, or PASSPORT.

BITS Admin Examples

The following examples demonstrate how to use the BITSAdmin tool to perform a specific task.

Creating a Job

To create a download job called mydownload job, perform the following steps:

1. Log on as an authorized administrator.
2. Click **Start**, select **Run**, type cmd, and then press **Enter**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. At the command prompt, type the following: bitsadmin /create /download myDownloadJob then press **Enter**.

Adding files to a Job

To add files to a download job, using the previously created job, mydownload, perform the following steps:

1. Log on as an authorized administrator.
2. Open a command prompt by clicking **Start**, click **Run**, type cmd, and press **Enter**.
3. At the command prompt, type the following: bitsadmin /addfile myDownloadJob http://exampleserver/bigfile.zip then press **Enter**.

Canceling a Job

To cancel the download job called mydownloadjob, perform the following steps:

1. Log on as an authorized administrator.
2. Open a command prompt by clicking **Start**, click **Run**, type cmd, and press **Enter**.
3. At the command prompt, type the following: bitsadmin /cancel myDownloadJob then press **Enter**.

Securing an IIS 6.0 host with the SCW

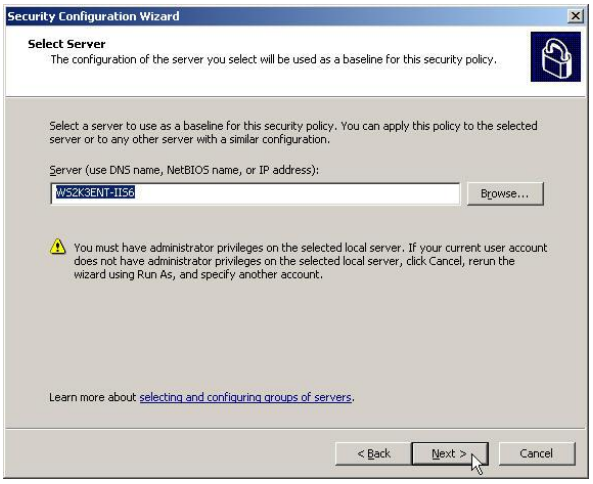
For information about the **SCW** see the Security Configuration Wizard subsection. To use the SCW to lockdown an IIS server host:

1. Log on as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Security Configuration Wizard**. The **Security Configuration Wizard** interface will be displayed. Click **Next**.

3. A list of action options will appear as shown below. Select the **Create a new security policy** radio button and click **Next**.

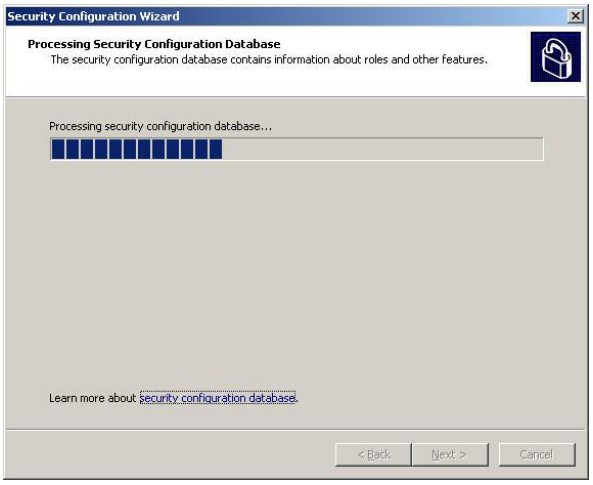
Copyright © 2008 Microsoft Corporation.
All rights reserved.

4. Select the server to be used as a baseline for the security policy applied by the SCW template. By default, the local machine name will be displayed. Click **Next**.

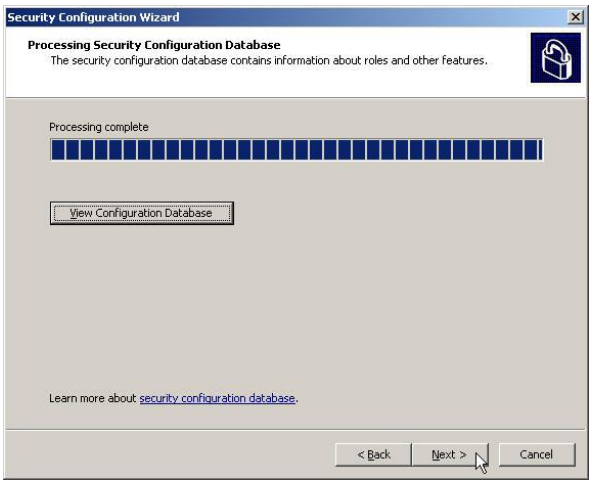


5. The SCW will begin scanning the server to build the security configuration database. The server is scanned to determine the following:
   - Server roles that are currently configured on the server;
   - Server roles that are likely being performed by the server;
   - Services that are installed but are not part of the Security Configuration Database; and
   - IP addresses and subnets that are configured for the server.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



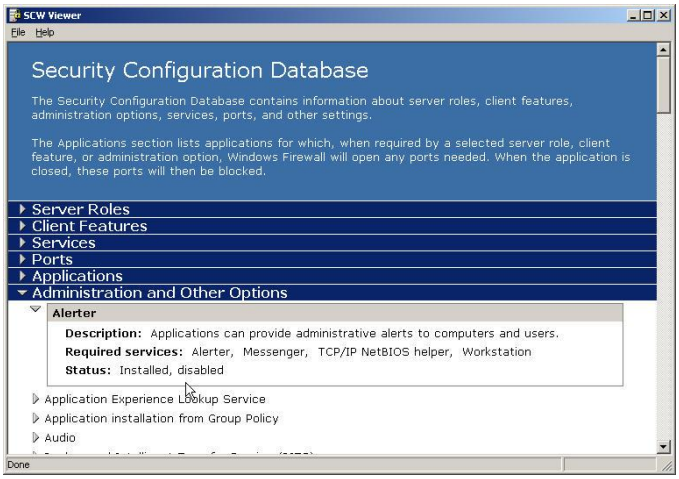
6. Click Next when the processing has been completed. If desired, click **View Configuration Database** to open the **SCW Viewer**.



7. The **SCW Viewer** displays information contained in the current **Security Configuration Database**. The information is presented in six categories: Server Roles, Client Features, Services, Ports, Applications, and Administration and Other Options. To view components within each category, click on the arrow head next to the category. Likewise, clicking the arrow head next to a category item provides a description of the item and its current setting status. When finished, close the **SCW Viewer**.

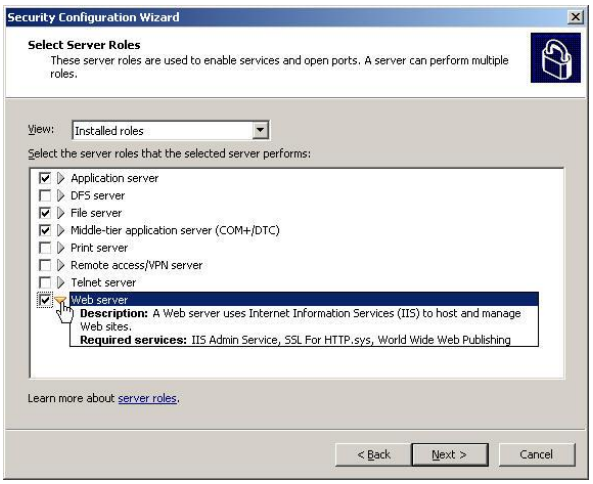
Copyright © 2008 Microsoft Corporation.

All rights reserved.



8. The **Role-Based Service Configuration** portion of the SCW will begin. Click **Next**.

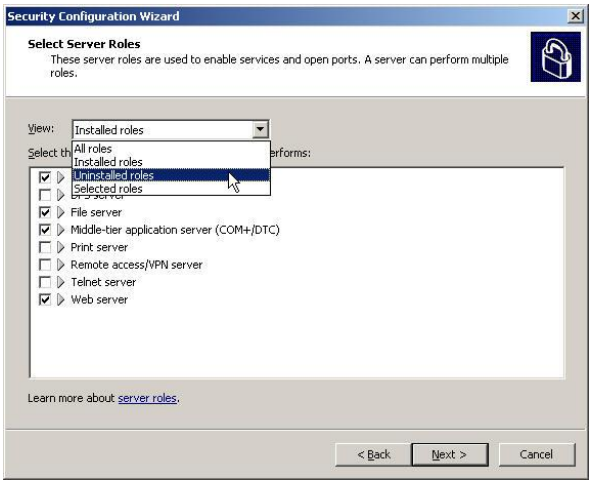
9. A list of server roles will be displayed. By default, the **Installed roles** view will be displayed. If IIS is already installed, the Web server role will appear on the list. Make sure its check box is selected.



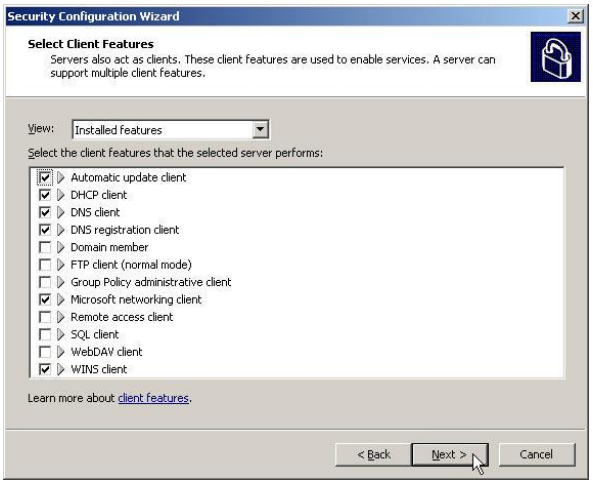
10. If IIS is not currently installed on the server, the **Web server** role may not be displayed in the list of **Installed roles**, select the **Uninstalled roles** view from the **View** drop-down menu. A list of server roles that are not currently installed will be displayed. Find the **Web server** role and select it.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



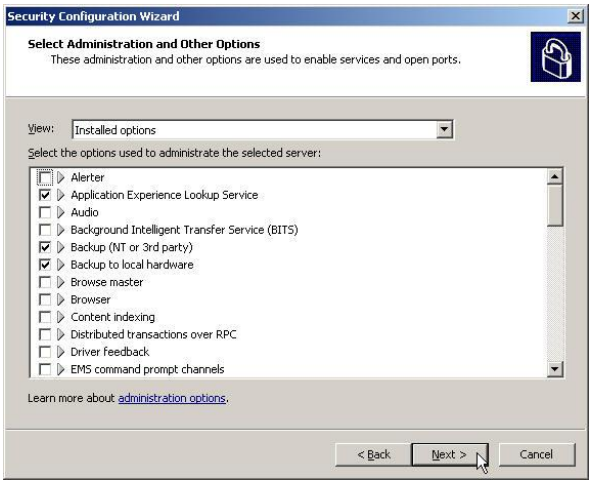
11. Click **Next** on the **Select Server Roles** page of the Wizard. A list of installed client feature will appear. Review the list and make any necessary changes. Deselecting a client feature will cause the SCW to disable it when it applies the completed policy. Selecting a client feature will allow the client feature to be used when the completed policy is applied. Click **Next** on the **Select Client Features** page of the Wizard.



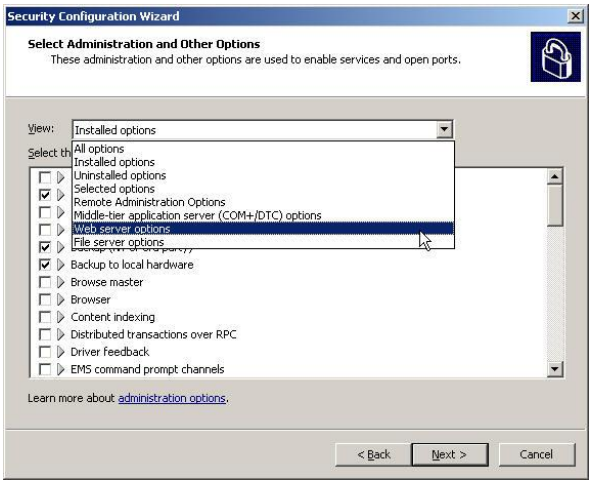
12. The Select Administration and Other Options page of the Wizard will display a list of installed administration service options discovered during the server scan. Those that are active will have check mark next to them. Select any additional services that need to be allowed by the SCW policy once it is applied.

Copyright © 2008 Microsoft Corporation.

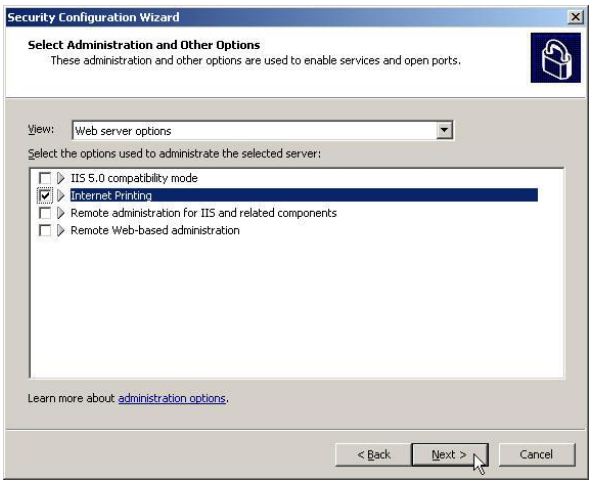
All rights reserved.



13. From the **View** drop-down menu, select Web server options.



14. Select any additional Web server options that need to be allowed by the SCW policy, such as **Internet Printing**, and click **Next**.



15. If any additional services were detected during the server scan, such as third-party application services, they will appear in the **Select Additional Services** page of the Wizard. Review the list, if any, and make appropriate changes. Click **Next** on the **Select Additional Services** page of the Wizard.

Copyright © 2008 Microsoft Corporation.

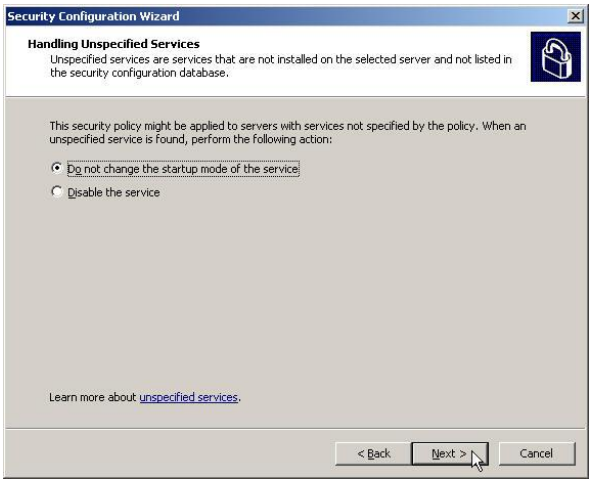
All rights reserved.

16. The **Handling Unspecified Services** page of the Wizard will appear. Review the information displayed and make the appropriate choice. Unspecified services are services that do not appear in the Security Configuration Database and are not currently installed on the selected server, but might be installed on other servers to which security policy may be applied. They might also be installed on the selected server at some point in the future. Use this page if it is necessary to do one of the following:

    - Apply the security policy to servers other than the selected server.
    - Apply the security policy to the selected server, but the selected server configuration has changed (for example, if new software is installed).

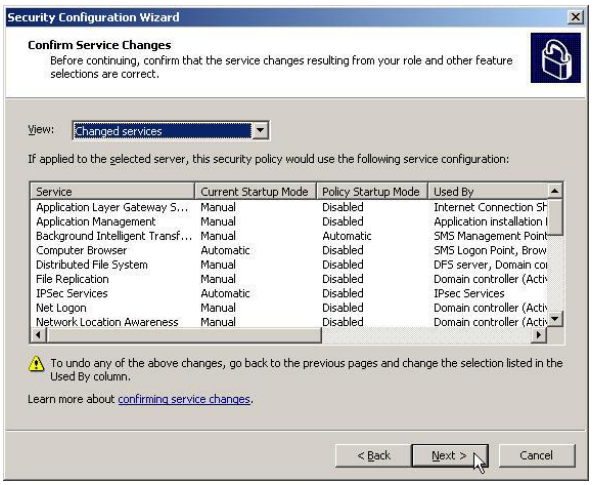
    The options are as follows:

    - **Do not change the startup mode of the service**. If this option is chosen, unspecified services that are enabled on servers to which this security policy is applied remain enabled, and those that are disabled remain disabled.
    - **Disable the service**. If this option is chosen, all services that are not in the Security Configuration Database or not installed on the selected server are disabled.



17. Click **Next** on the **Handling Unspecified Services** page of the Wizard.

18. The **Confirm Service Changes** page will display all changes that will be made by the SCW policy on the scanned host configuration. Review the changes. To make any edits, use the **Back** button to find the correct page on which to make the correction. Click **Next** on the **Confirm Service Changes** page of the Wizard.

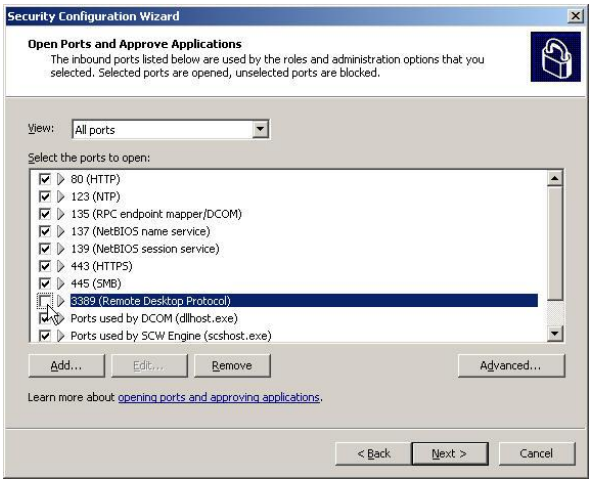


Copyright © 2008 Microsoft Corporation.

All rights reserved.

19. The **Network Security** configuration portion of the SCW will begin. This section of the SCW configures the **Windows Firewall**. Advanced options in this section configure **Internet Protocol security (IPSec)**. There is an option to **Skip this section** if desired. However, if this section is skipped, the Windows Firewall and IPSec settings will not be configured. By default, the **Skip this section** check box is selected. Deselect the **Skip this section** check box to configure the Windows Firewall and IPSec setting, then click **Next**.

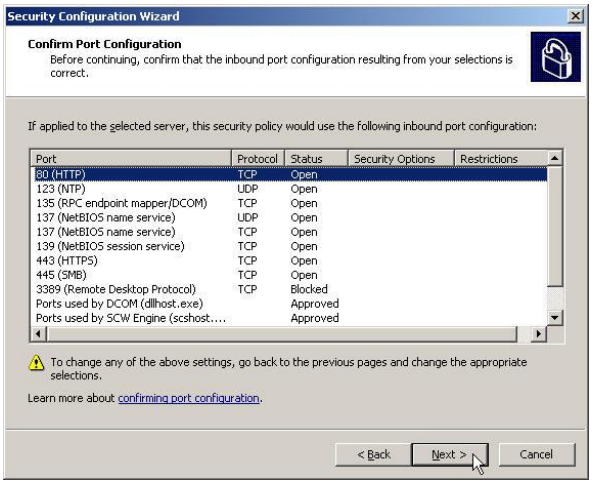
20. The **Open Ports and Approve Applications** page of the Wizard shows a list of ports identified during the server scan. Each entry in the ports list is shown with a check box, a triangular arrow that can be clicked for more information about the port, and either the port number with a description or the application. Initially, the required check boxes are selected because the ports are presumed to be required, but they can be cleared in order to block those ports. Optional ports, which may be needed for backward compatibility, are not selected by default. This page can be used to add ports, edit port numbers and protocols, or remove ports with the **Add**, the **Edit** and the **Remove** buttons. The buttons are unavailable as appropriate. For example, if port number and protocol are fixed, the **Edit** button is unavailable. Use the **Advanced** button to create, or change, local or remote restrictions on a selected port. When all appropriate port changes are made, click **Next**.



21. The **Confirm Port Configuration** page of the Wizard is displayed. This page summarizes the resulting port configuration settings. If a setting is not correct, click **Back** to get to the incorrect setting and then change it. If the settings are correct, click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

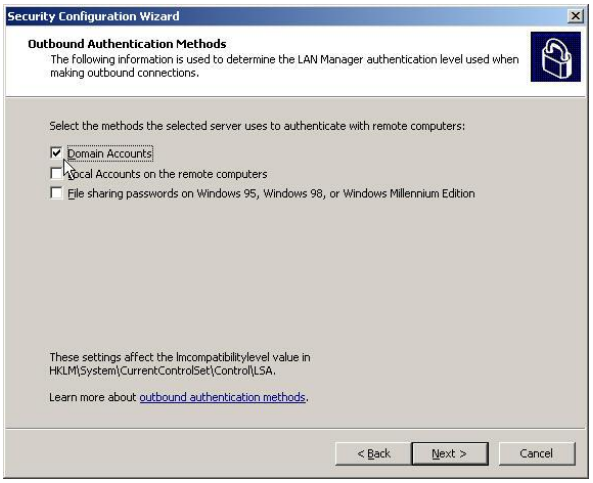


22. The **Registry Settings** configuration portion of the SCW will begin. This section of the SCW secures registry settings that support communications with other computers. Click **Next**.

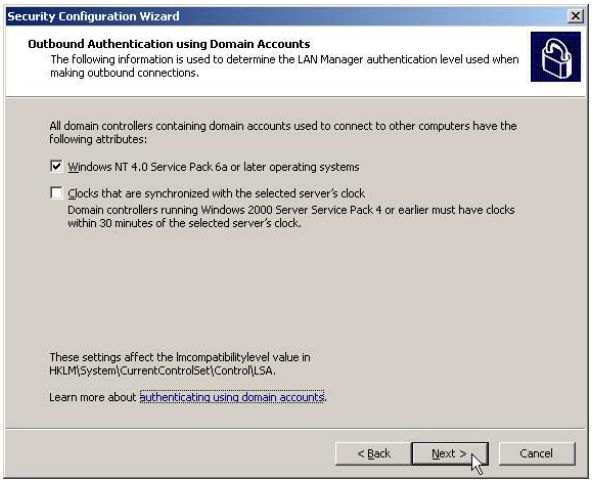
23. The **Require SMB Security Signatures** page of the Wizard is displayed. This page is used to specify whether the SMB communications protocol should have security signatures enabled or required. Make appropriate selections and click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

24. The **Outbound Authentication Methods** page of the Wizard is displayed. On this page, information is gathered about the accounts used by the selected server to authenticate to other computers. Make appropriate selections and click **Next**.



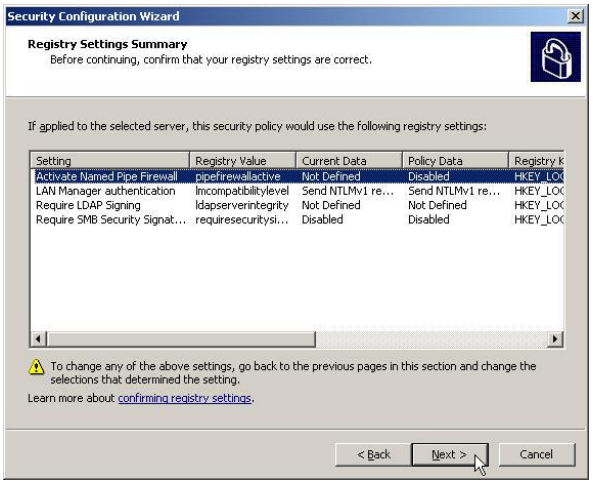
25. Depending on the choices made above, the **Outbound Authentication using Domain Accounts** and/or the **Outbound Authentication using Local Accounts** pages of the Wizard may be displayed. Both pages have similar choices. Make appropriate selections and click **Next**.



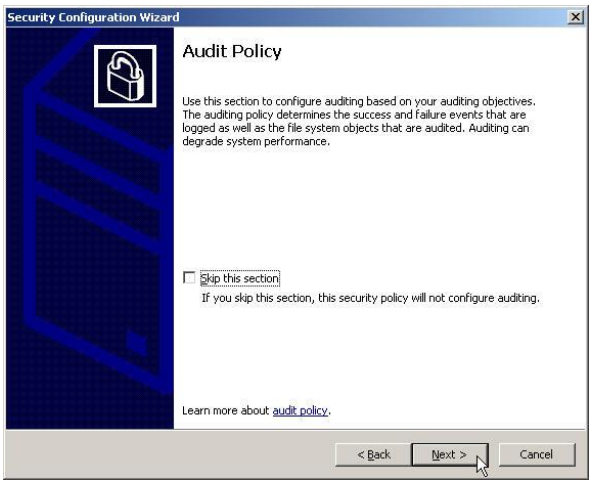
26. The **Registry Settings Summary** page of the Wizard is displayed. This page provides a review of the changes that this security policy would make to specific registry settings if applied to the selected server. The SCW shows the current setting for each registry value and the setting value defined by the policy. No changes are made to the selected server until the security policy is applied. If a setting is not correct, click **Back** to get to the incorrect setting and then change it. If the settings are correct, click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



27. The **Audit Policy** configuration portion of the SCW will begin. This section provides general background information about the Audit Policy section of the SCW. It allows authorized administrators to specify whether the Widows audit policy will be modified to change the level of logging on the selected server. Click **Next**.

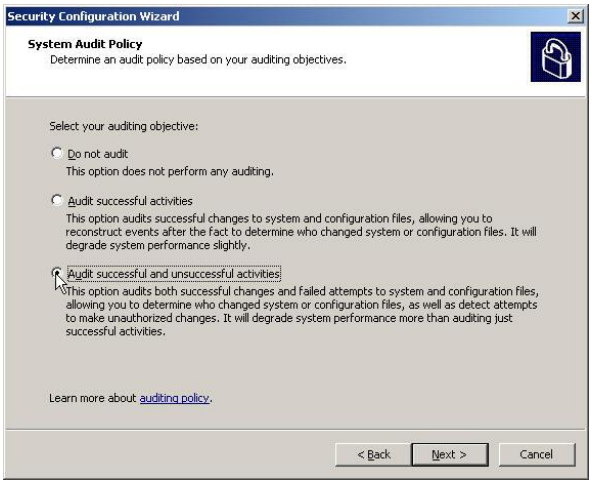


28. The **System Audit Policy** page of the Wizard is displayed. This page is used to create an audit policy for servers in the organization. Auditing is the process that tracks the activities of users and records selected types of events in the security log. Select the **Audit successful and unsuccessful activities** radio button and click **Next**.

Note: If **Audit successful activities** is selected, then unauthorized intrusion attempts will not show up in the log. Unauthorized intrusion attempts are characterized by large numbers of unsuccessful activities.

Copyright © 2008 Microsoft Corporation.

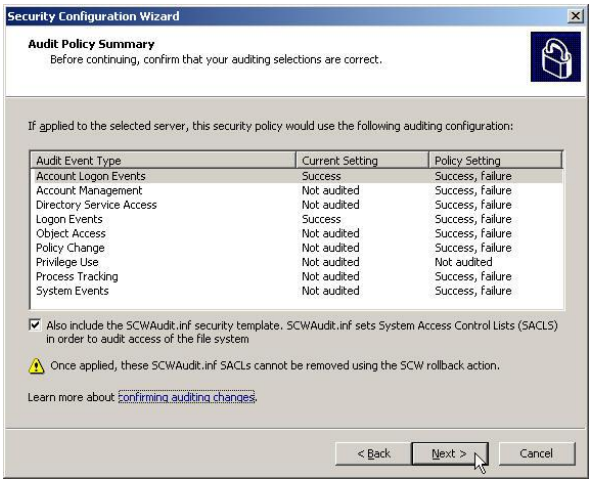
All rights reserved.



29. The **Audit Policy Summary** page of the Wizard is displayed. This page provides a list of all of the changes that will be made to the audit policy on the selected server if the policy is applied. It shows the current setting for each audit policy setting and the setting defined by the policy. No changes are made to the selected server until the security policy is applied.

    There is a check box which provides the option of including the ASCaudit.inf security template. In ASCaudit.inf, the SACLs aid in the detection of tampering or attempted tampering to the operating system. These SACLs enable the system to record write access by any user to any executable or configuration files in the Windows directory structure, and changes to the state or configuration of Windows services. The SACLs do not cause Windows to monitor files and directories that are primarily used for other purposes, and they generate as few logged events as possible, so that they do not overwhelm administrators. However, application of a service pack, restoring information from a backup, or changing permissions on all or part of the Windows directory could result in a large number of events being generated. The SCW rollback feature does not include the ability to roll back SACLs. Therefore, the **Audit Policy Summary** page allows the option of not applying the ASCAudit.inf security template.

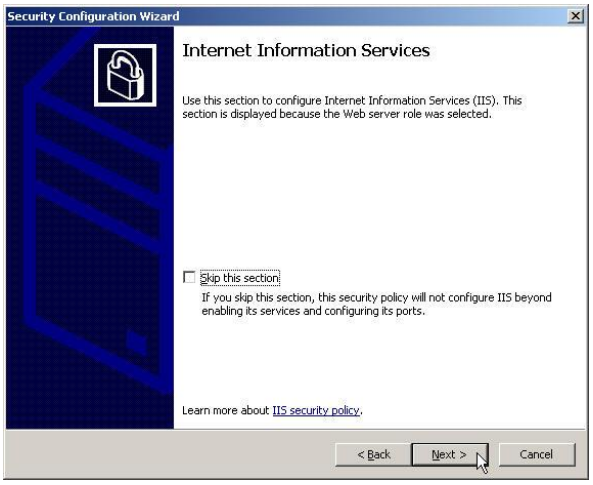
    Click **Next**.



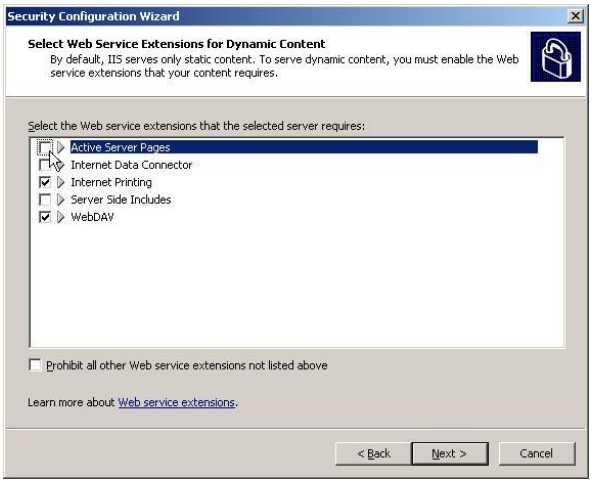
30. The **Internet Information Services** configuration portion of the SCW will begin. This configuration portion appears because the **Web server** role was selected for this SCW policy. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



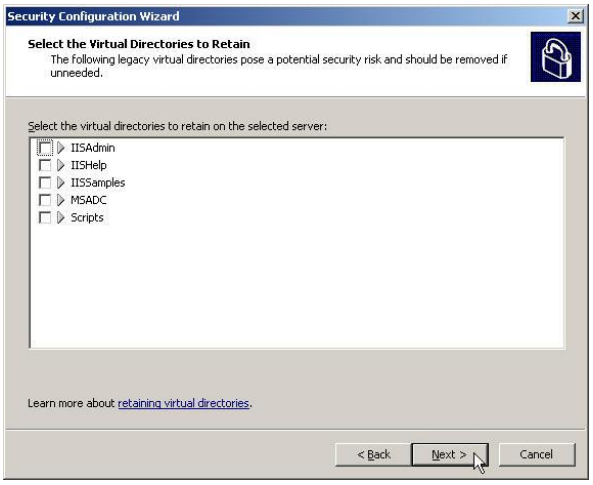
31. The **Select Web Service Extensions for Dynamic Content** page of the Wizard is displayed. A Web service extension is a request handler for a specific content type. For example, when a Web server receives a request for ASP content, a Web service extension is called to serve the ASP content to the client's browser. ASP is not allowed for the Evaluated Configuration. Therefore, deselect the **Active Server Page** check box and click **Next**.



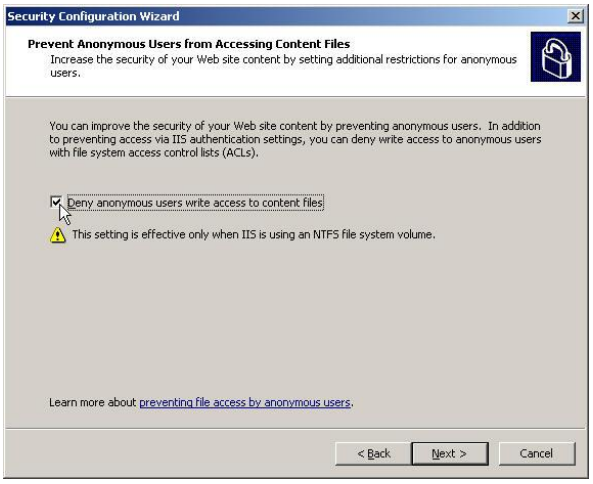
32. The **Select the Virtual Directories to Retain** page of the Wizard is displayed. This page allows the option of retaining or removing virtual directories that are configured on the Web server by default. Do not select any of the default virtual directories for retention. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



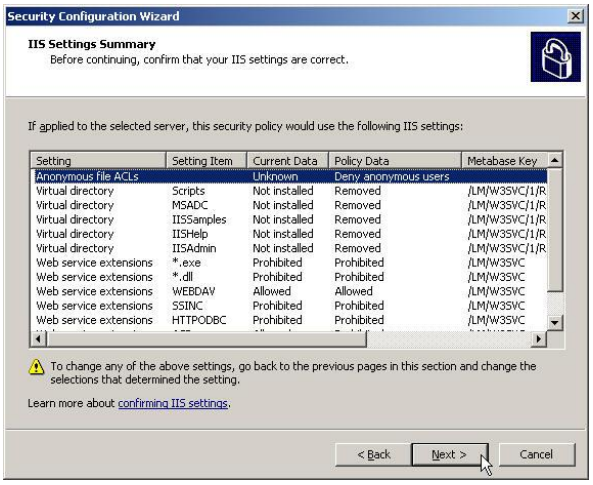
33. The **Prevent Anonymous Users from Accessing Content Files** page of the Wizard is displayed. This page allows authorized administrators to create a policy that denies anonymous users write access to content files on the Web site. Check the **Deny anonymous users write access to content files** check box and click **Next**.



34. The **IIS Settings Summary** page of the Wizard is displayed. This page provides the opportunity to see all of the changes that this security policy will make to specific IIS settings on the selected server. The SCW shows the current setting for each IIS setting and the setting value defined by the policy. No changes are made to the selected server until the security policy is applied. If a setting is not correct, click **Back** to get to the incorrect setting and then change it. If the settings are correct, click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



35. The **Save Security Policy** portion of the SCW will begin. Click **Next**.

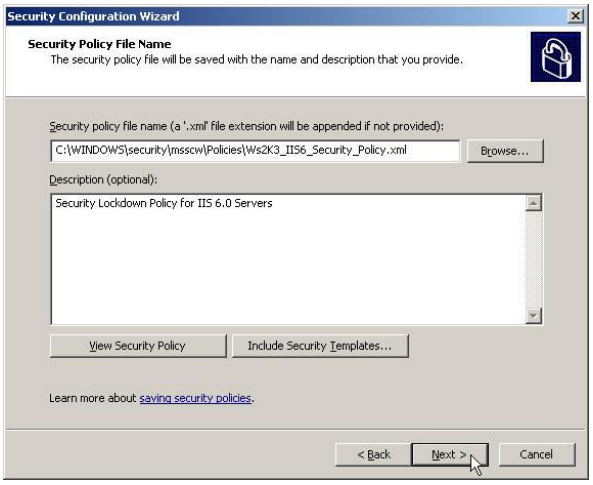
36. The **Security Policy File Name** page of the Wizard is displayed. Choose a location and a file name with an .xml extension for saving the security policy. The policy can be saved on the local hard disk, or in a network shared folder, in a location accessible to administrators who will run the SCW to apply the policy.

    Security policies that are created with the SCW include some, but not all possible security policy settings. If needed, use the **Include Security Templates** button to access a dialog box that allows selection of a security template with to be included with the SCW security policy. If some template settings conflict with SCW, then SCW settings will take precedence.

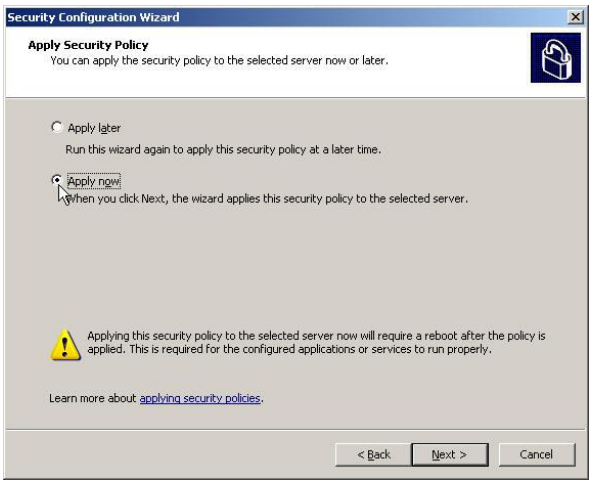
    Click **Next**.

Copyright © 2008 Microsoft Corporation.

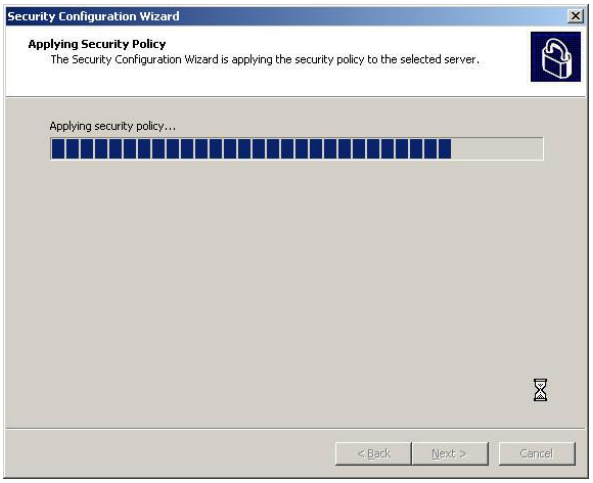
All rights reserved.



37. The **Security Policy File Name** page of the Wizard is displayed. Select to either apply the security policy now to the current server or to apply it at a later time. Click **Next**.



38. If the **Apply now** option was selected, the SCW will begin applying the security policy to the server. When it is finished, click **Next**.



39. The **Completing the Security Configuration Wizard** page of the SCW will be displayed. Click **Finish** to complete the Wizard.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: The **Windows Firewall** is turned off by default in a Windows Server 2003 installation. If firewall settings were configured by the SCW, the **Windows Firewall** will be turned on and will be configured with the firewall rules specified by the SCW.

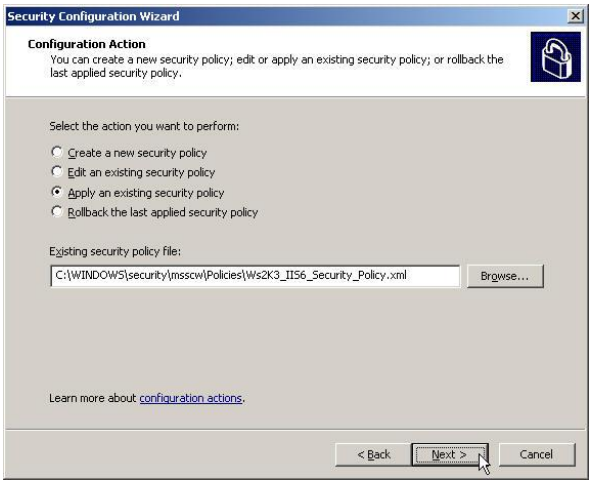
Applying the SCW Security Policy

To apply the previously defined SCW policy to a Windows Server 2003 IIS 6.0 host, copy the .xml policy file to the host and follow the procedures below.

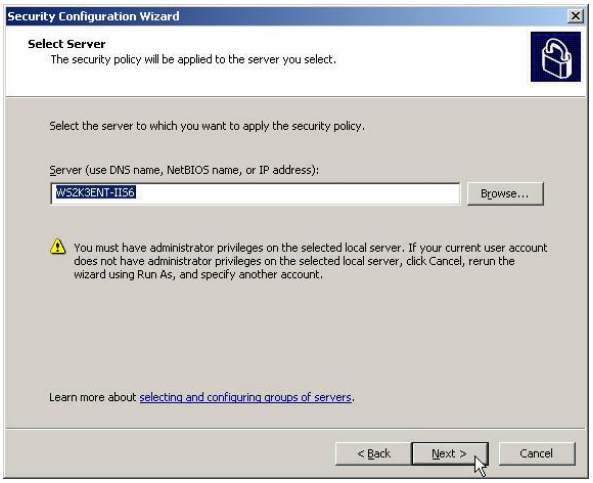
1. Log on as an authorized administrator.
2. Click on **Start**, point to **Administrative Tools**, and then select **Security Configuration Wizard**. The **Security Configuration Wizard** interface will be displayed. Click **Next**.

3. Select the **Apply an existing security policy** radio button. Click the **Browse** button and find and select the .xml SCW policy file, then click **Next**.

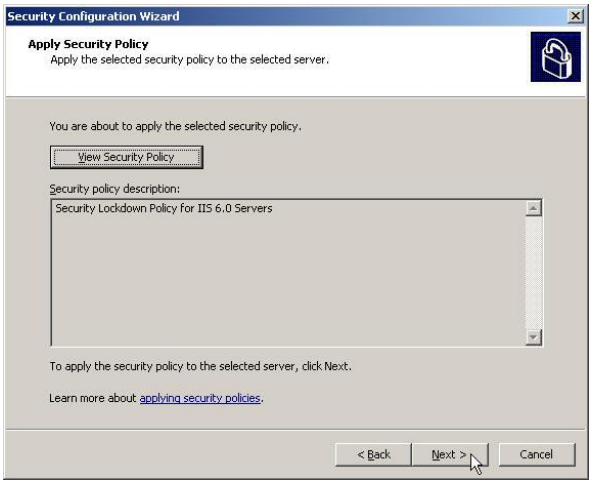
Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. In the **Select Server** page of the SCW, enter the name of the server on which the policy will be applied. The local machine name will be the default. User the **Browse** button if needed to find the server on the network. Click **Next**.



5. The **Apply Security Policy** page of the SCW will be displayed. If desired, click the **View Security Policy** button to review the security policy settings that will be applied. Click **Next**.



6. The SCW will begin applying the security policy to the server. When it is finished, click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

7. The **Completing the Security Configuration Wizard** page of the SCW will be displayed. Click **Finish** to complete the Wizard.

Note: The **Windows Firewall** is turned off by default in a Windows Server 2003 installation. If firewall settings were configured by the SCW, the **Windows Firewall** will be turned on and will be configured with the firewall rules specified by the SCW.

Implementing Active Directory Federation Services

Active Directory Federation Services (ADFS) enables federated identity and access management by securely sharing digital identity and entitlement rights across security and enterprise boundaries by enabling organizations to securely share a user's identity information over *federation*[6] trusts. ADFS creates a cryptographically-signed security token to represent a user session. The token can be based on public key certificate, Kerberos, or Security Assertion Markup Language (SAML). The token is used for single sign-on across distributed, trusted portions of the TOE, authenticating and authorizing users for the controlled access of Web resources.

Understanding Active Directory Federation Services

Active Directory in Windows Server 2003 R2 with SP2 provides the benefit of functionality through Windows-integrated authentication within the organization's security or enterprise boundaries. ADFS extends this functionality across forest trusts and to external network-facing applications. This enables customers, partners, and suppliers to have a similar Web Single-Sign-On (SSO) user experience when they access the organization's Web-based applications. Furthermore, federation servers can be deployed in multiple organizations to facilitate business-to-business (B2B) federated transactions between partner organizations.

When an application is enabled for federated user access, users both within an organization and at organizations that have configured a federation trust to that organization can access the ADFS-enabled application that is hosted by that organization.

[6] A pair of realms or domains that have established a federation trust.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Note: Although ADFS can extend single sign-on functionality to external network-facing applications, accessing ADFS-enabled applications over the Internet, access to the Internet is not supported in the TOE.

The topics in this section include:

- Partner organizations
- Federation trusts
- ADFS components and server roles
- Types of ADFS-aware Web applications
- ADFS scenarios
- Certificates used by ADFS
- Cookies used by ADFS

Partner Organizations

The Federated Web SSO scenario involves two types of partner organizations – an account partner and a resource partner. For the purposes of this guide, the local network that contains the resources to be accessed by the users located in the account partner's network is referred to as the *resource realm* (or resource domain). The network that contains the Active Directory accounts belonging to external users that access the resources on the internal network is referred to as the *account realm* (or account domain). The federation servers for each respective partner organization are differentiated as the *account federation server* and the *resource federation server*.

Account partner

An account partner represents the organization in the federation trust relationship that physically stores user accounts in an Active Directory store. The account partner is responsible for collecting and authenticating a user's credentials, building up claims for that user, and packaging the claims into security tokens. These tokens can then be presented across a federation trust to access Web-based resources that are located in the resource partner organization.

In other words, an account partner represents the organization for whose users the Federation Service issues security tokens. The Federation Service in the account partner organization authenticates local users and creates security tokens that are used by the resource partner in making authorization decisions.

In relation to Active Directory, the account partner in ADFS is conceptually equivalent to a single Active Directory forest whose accounts need access to resources that are physically located in another forest. Accounts in this forest can access resources in the resource forest only when an external trust or forest trust relationship exists between the two forests and the resources to which the users are trying to gain access have been set with the proper authorization permissions.

Note: This analogy is meant strictly to emphasize how the relationship between account and partner organizations in ADFS is similar, in concept, to the relationship between an account forest and a resource forest in Active Directory. External trusts and forest trusts are not required for ADFS to function.

As an account partner, the Federation Service allows Active Directory users to access resources at partner organizations. In response to a request from a resource partner, the Federation Service collects and verifies user credentials against Active Directory. The Federation Service can then populate a set of organization claims based on the Lightweight Directory Access Protocol (LDAP) attributes of the user account. The organization claims are then mapped to appropriate claims for the resource partner and

Copyright © 2008 Microsoft Corporation.

All rights reserved.

packaged into a security token that is signed by the Federation Service's token-signing certificate. The resultant security token is posted as the response to the resource partner's original request. The resource partner then uses the token to allow access for the user.

Resource partner

The resource partner is the other organizational partner in the federation trust relationship. A resource partner administers the Web servers that host ADFS-enabled applications. The resource partner organization trusts its account partner to authenticate users. To make authorization decisions, the resource partner consumes the claims that are packaged in security tokens coming from the account partner.

To function as an ADFS resource, Web servers in the resource partner organization must have the ADFS Web Agent component of ADFS installed. Web servers that are secured by ADFS can host claims-aware applications or Windows NT token-based applications.

In relation to Active Directory, the resource partner is conceptually equivalent to a single forest whose resources are made available over an external trust or forest trust relationship to accounts that are physically stored in another forest.

As a resource partner, the Federation Service plays the opposite role of the account partner. When a user attempts to access an ADFS-enabled application, the Federation Service determines which account partner should authenticate the user. It then sends an authentication request to that partner. When the user returns with a security token, the Federation Service verifies that the token has been correctly signed by the partner. It then extracts the claims from the token. The claims are mapped to organization claims, and the filtering policy for the specific application is applied. The filtered organization claims are packaged into a security token that is either signed by the Federation Service's token-signing certificate or protected by a Kerberos session key for the Web application. The resultant security token is posted back to the original application Uniform Resource Locator (URL). The application then uses the token to allow access for the user.

Note: Account partners and resource partners are not used in the Web SSO scenario (to be described in more detail later in this guide).

Federation Trusts

A *federation trust* is the embodiment of a business-level agreement or partnership between two organizations. The Federated Web SSO scenario may or may not include a federation trust in its configuration. For the purposes of the Common Criteria evaluation, the Federated Web SSO scenario demonstrated in the TOE includes a federation trust (but is not configured to use a forest trust).

The ADFS administrator can establish federation trust relationships between two partner organizations. A federation trust is created when the account partner organization and the resource partner organization both install the Federation Service component of ADFS and they both use the Active Directory Federation Services snap-in to configure the account partner and resource partner appropriately. Authentication flows from the account partner organization to the resource partner organization.

After the federation trust is created, users who are located in the account partner organization can send authentication requests successfully through the federation trust to the Web server in the resource partner organization.

Note: Federation trusts are not used in the Web SSO scenario.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

ADFS Components and Server Roles

Active Directory Federation Services (ADFS) has three components:

- **Federation Service:** Functions as a security token service and routes authentication requests from external user accounts.
- **Federation Service Proxy:** Functions as a proxy for the Federation Service in a perimeter network. This component is optional in an ADFS deployment.
- **ADFS Web Agent:** Provides authorization (consumes security tokens) and either allows or denies access to two types of Web applications, as follows:
  - **Claims-aware applications:** Makes authorization decisions based on claims.
  - **Windows NT token-based applications:** Uses Windows-based authorization mechanisms.

A server running an ADFS component performs one of the three following server roles, as described in detail in this section:

- Federation server
- Federation server proxy
- Web server

Federation server

Federation servers host the Federation Service component of ADFS. They are used to route authentication requests that are made from user accounts in other organizations (in Federated Web SSO scenarios) or from clients that can be located in an external network (in the Web SSO scenario).

Federation servers also host a security token service that issues tokens that are based on the credentials (for example, user name and password) that are presented to it. After the credentials are verified (by the user typing in a user name and password, for example), claims for the user are collected through examination of the attributes for the user that are stored in Active Directory.

In the Federated Web SSO scenario, the role that a federation server plays depends on whether the organization is designated as the account partner or the resource partner. For more information, see the Partner organizations section earlier in this guide.

Federation server proxy

Federation server proxies host the Federation Service Proxy component of ADFS. Federation server proxies can be deployed in an organization's perimeter network to forward requests to federation servers that are not accessible from the external network.

> **Note:** Although separate servers can be deployed to host the Federation Service Proxy component, it is not necessary to deploy a separate server to act as a federation server proxy in the intranet forest of either the account partner or the resource partner. A federation server performs this role automatically.

In the Federated Web SSO scenario, the role that a federation server proxy plays depends on whether the organization is the account partner or the resource partner:

- Federation Service Proxies at the account partner act as proxies for user logons to federation servers that are located in the internal network. Federation server proxies also act as proxies for security tokens that are issued by the account partner federation server for its tokens and tokens that are destined for resource partners.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Federation Service Proxies in the resource partner act as proxies for user security tokens, which are issued from federation servers in both the account partner and the resource partner, to Web-based applications in the resource partner's realm.

In the Web SSO scenario, a federation server proxy prevents external clients from directly accessing internal federation servers. This isolates the federation servers so that they can be accessed only by clients that are logged on to the local network and through federation server proxies, which act on behalf of external clients. Federation server proxies do not have access to the keys that are used to produce tokens.

Web server

In ADFS, Web servers in the resource realm host the ADFS Web Agent component to provide secure access to the Web applications that are hosted on those Web servers. The ADFS Web Agent manages security tokens and authentication cookies that are sent to a Web server. The Web server requires a relationship with a Federation Service so that all authentication tokens come from that Federation Service.

The ADFS Web Agent supports two types of applications: claims-aware applications and Windows NT token–based applications. These are described in the next section.

Types of ADFS-aware Web Applications

There are two types of Web-based applications that are ADFS-aware:

- Claims-aware applications
- Windows NT token-based applications

Claims-aware applications

Claims-aware applications are Microsoft ASP.NET 2.0 applications that are written so that they can query ADFS security token claims. When the Web-based application used in the TOE is a claims-aware application, the ADFS Web Agent that is running on the Web server does not have to create Windows NT security tokens for the user. Federated applications that are claims-aware should be developed specifically to use the claims that are produced by ADFS. When an application is presented with a valid token, the claims-aware application can make authorization decisions based on the claims in the token, which stores all the information about a given identity. The application might store additional information that links to the identity that is presented in the token, but a user account in Active Directory on the local domain is not required to access a claims-aware application.

In the Federated Web SSO scenario, when incoming claims are received by the resource federation server from the account federation server, they are mapped to organization claims on the resource federation server. In the procedures provided by this guide, security groups in Active Directory are used to demonstrate claims mappings in ADFS.

The following list describes the organization claims that can be used by claims-aware applications:

- **Identity claims (UPN/e-mail/common name)**. When configuring the application, specify which of these identity claims will be sent to the application. No mapping or filtering is performed.
- **Group claims**. When configuring the application, specify the organization group claims that are sent to the application. Organization group claims that are not designated to be sent to the application are discarded.
- **Custom claims**. When configuring the application, specify the organization custom claims that are sent to the application. Organization custom claims that are not designated to be sent to the application are discarded.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Windows NT token-based applications

Windows NT token–based applications are IIS applications that are written to use Windows-based authorization mechanisms. These applications require Windows NT security tokens to make authorization decisions. ADFS can enable the transition of an ADFS security token to an impersonation-level Windows NT access token.

With a Windows NT token–based application, claims in incoming ADFS tokens are mapped to either user accounts or groups in the local Active Directory user store in the resource realm. The user accounts or groups are also known as *resource accounts* or *resource groups*. The application then uses the resource accounts or groups to perform authorization.

Resource account mapping is required with federated Windows NT token-based applications because the ADFS Web Agent must reference an Active Directory security principal in the resource partner forest to build the Windows NT access token and thereby enforce access control on the application. Resource groups can be used to map multiple federated users to a single Active Directory security group.

Claims-aware applications do not require resource account mapping because they use the ASP.NET membership and roles model, which means they can inherently consume User Principal Names (UPNs) and group claims directly from the ADFS security token.

When a client makes a request to a Windows NT token-based application, the ADFS Web Agent that is running on the Web server intercepts the request and creates Windows NT security tokens, which are required by the Web application to make authorization decisions. For users in the resource realm, this is possible because the Web server that hosts the Windows NT token-based application is joined to the resource domain. For users in the account realm (or for external users in the Web SSO scenario), this is enabled through mapped resource groups.

ADFS Scenarios

The two ADFS scenarios included in the TOE for Windows Server 2003 R2 with SP2 are as follows:

- Federated Web single sign-on (SSO)
- Web SSO

Federated Web SSO

The *Federated Web SSO* scenario involves two Active Directory forests in separate organizations. Each forest is located on a separate network, as depicted in Figure 3.1. Federation servers are deployed in both networks. A federation trust is established so that accounts can be used to access a Web-based application in the resource realm network, regardless of which forest the accounts accessing the Web site reside in.

If the Web application is a Windows NT token-based application, the ADFS Web Agent that is running on the Web application server intercepts requests and creates Windows NT security tokens, which are required by the Web application to make authorization decisions. For users in the resource realm, this is possible because the Web server that hosts the Windows NT token-based application is joined to the resource domain. For users in the account realm, this is enabled through mapped resource groups.

If the Web-based application is a claims-aware application, the ADFS Web Agent that is running on the Web server does not have to create Windows NT security tokens for the user. The ADFS Web agent can expose the claims that come across, which allows the application to make authorization decisions based on the contents of the security token that is provided by the account federation server.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

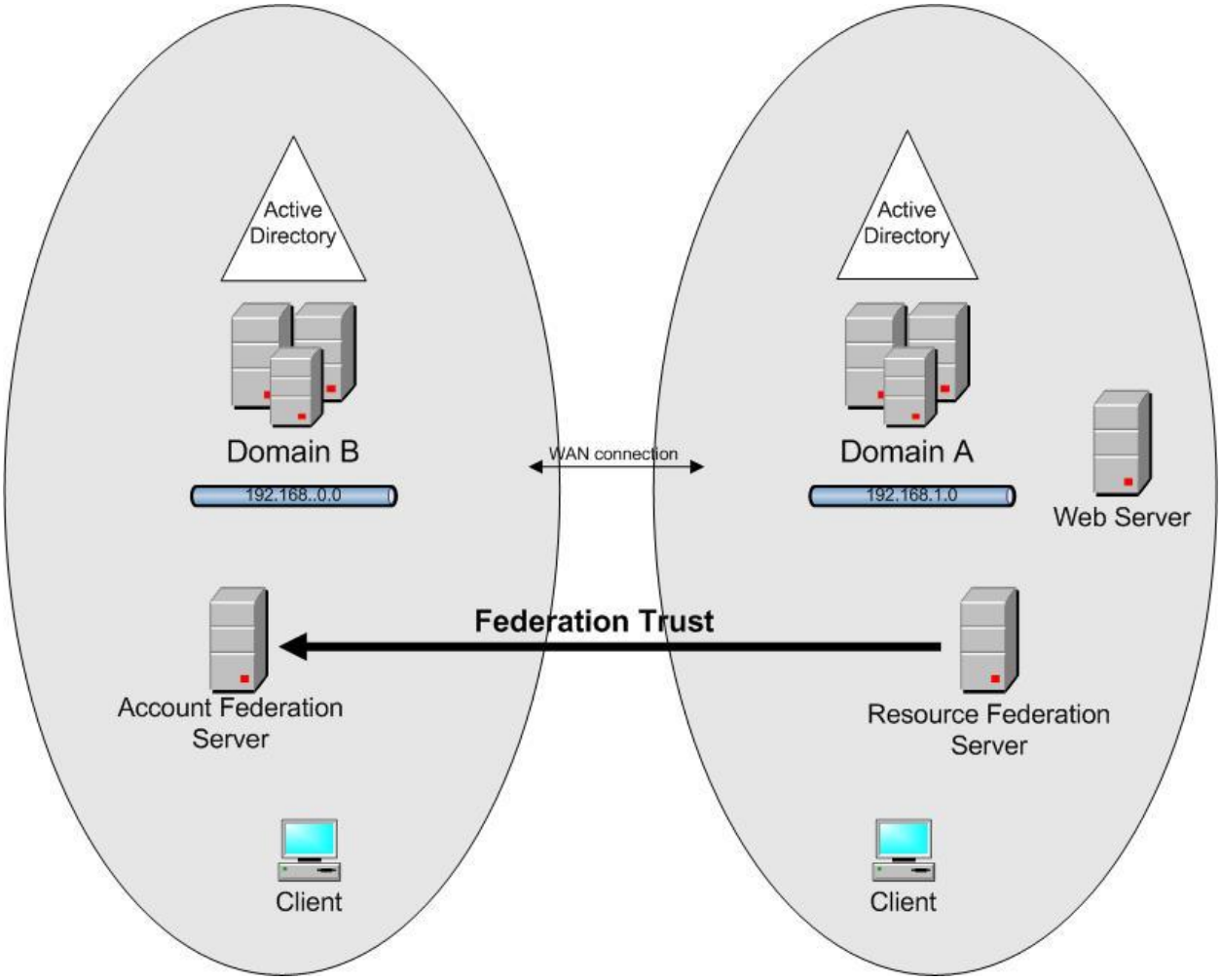


Figure 3.1 Overview of typical Federated Web SSO scenario

Web SSO

In the *Web SSO* scenario, remote users authenticate only once to access multiple Web-based applications on a protected network. Typically, in this scenario all users are external, and no federation trust exists, as depicted in Figure 3.2. Because the Web servers must be accessible from external network environments and also joined to the local Active Directory domain, they are connected to two networks; that is, they are multi-homed.

The first network is the perimeter network, which provides the needed connectivity for external clients. The second network (the protected network) contains the Active Directory forest, which is not directly accessible to external clients. The federation server proxy is also multi-homed to provide the necessary connectivity to the federation server and accessibility to external clients. In this scenario, placing the federation server on a network that is not directly accessible by external clients greatly reduces the risk to the federation server.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

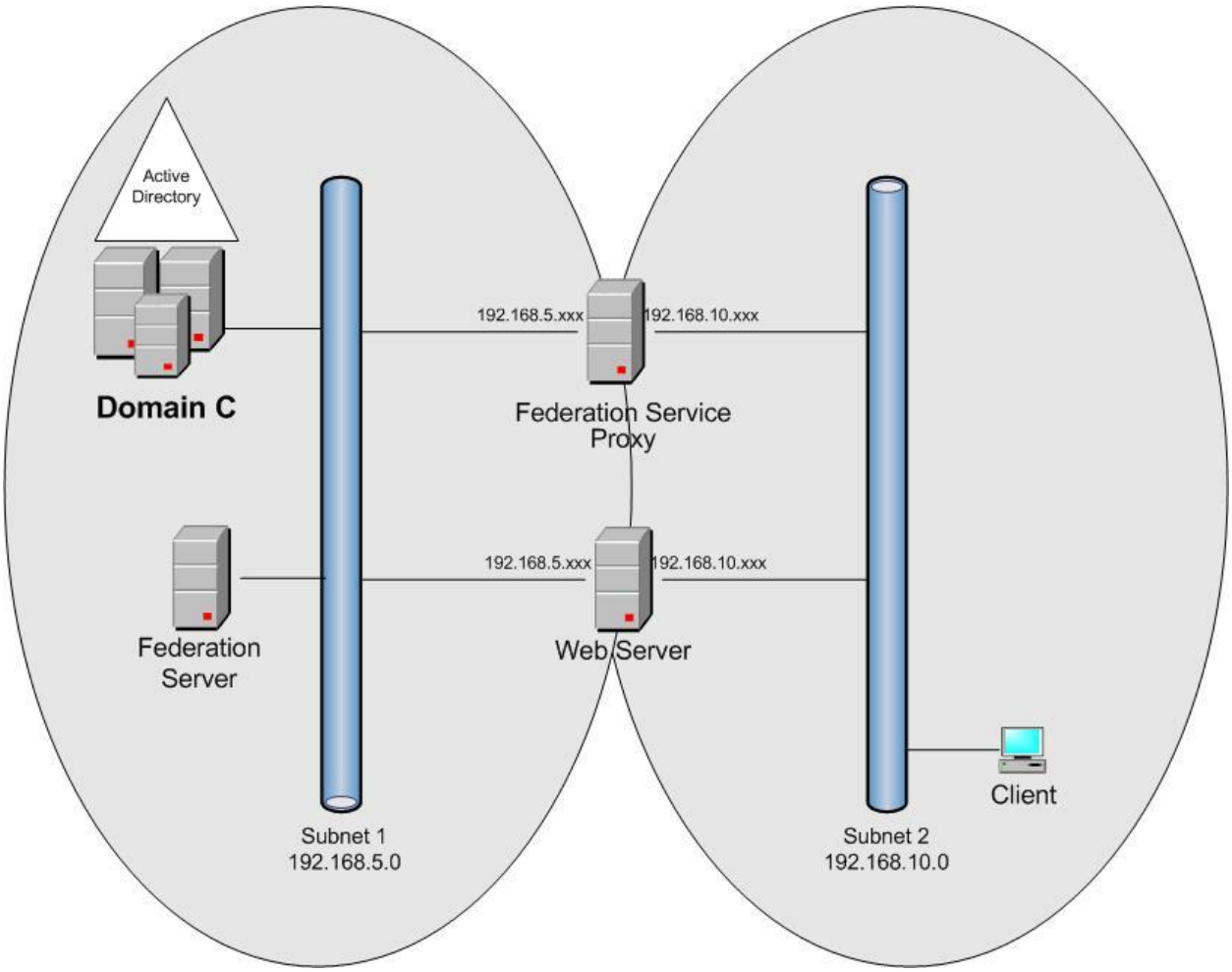


Figure 3.2 Overview of typical Web SSO scenario

Certificates Used by ADFS

Federation servers use the following types of certificates:

- Token-signing certificates
- Verification certificates
- SSL server authentication certificates
- Client authentication certificates

Token-signing certificates

Each federation server uses a *token-signing certificate* to digitally sign all security tokens that it produces. Because each security token is digitally signed by the account partner, the resource partner can verify that the security token was issued by the account partner and that it was not modified. This helps prevent attackers from forging or modifying security tokens to gain unauthorized access to resources.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Digital signatures on security tokens are also used within the account partner when more than one federation server is used. In this situation the digital signatures verify the origin and integrity of security tokens that are issued by other federation servers within the account partner. The digital signatures are verified with verification certificates.

Note: Each token-signing certificate contains a private key that is associated with the certificate.

Verification certificates

Verification certificates are used to verify that a security token was issued by a valid federation server and that it was not modified. Verification certificates are actually the token-signing certificates of other federation servers.

To verify that a security token was issued by a given federation server and not modified, the federation server must have a verification certificate for the federation server that issued the security token. For example, if federation server A issues a security token and sends the security token to federation server B, federation server B must have a verification certificate (federation server A's token-signing certificate) for federation server A.

Note: Unlike a token-signing certificate, a verification certificate does not contain the private key that is associated with the certificate.

Server authentication certificates

The federation server uses Secure Sockets Layer (SSL) *server authentication certificates* to secure Web services traffic for communication with Web clients or the federation server proxy. These certificates are requested and installed through the Internet Information Services (IIS) Manager console.

Client authentication certificates

The federation server proxy is the only type of federation server that uses a Secure Sockets Layer (SSL) *client authentication certificate*. The client authentication certificate is used for TLS/SSL communication with the Federation Service. The public portion of the Federation Service Proxy client authentication certificate is added to the trust policy on the federation server so that the Federation Service can authenticate the federation server proxy.

Cookies Used by ADFS

Active Directory Federation Services uses three types of cookies:

- Authentication cookie
- Account partner cookie
- Sign-out cookie

Authentication cookie

Authentication cookies can be issued by both the Federation Service and the ADFS Web Agent. The ADFS Web Agent takes the ADFS security token that it receives and uses that token as the cookie value.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The benefit at the Web server is that it does not need keying material. The Federation Service publishes all the information that is necessary to validate its tokens.

At the Federation Service, the security token in a cookie holds the organization claims for the client. The organization claims can be mapped to outgoing claims for a particular resource. The ADFS Web Agent can also authenticate and use cookies that are issued by the Federation Service. The Web server receives a cookie when the client accesses the Web server. Then, the ADFS Web Agent authenticates this cookie and uses the claims that it contains.

The authentication cookie facilitates single sign-on. After the Federation Service validates the client one time, the authentication cookie is written to the client. The Federation Service produces and consumes the contents of the authentication cookie, and they are opaque to federation server proxies. Further authentication takes place through use of the cookie rather than through repeated collection of the client credentials.

The authentication cookie is always a session cookie. The authentication cookie is signed but not encrypted, which is one reason why use of Transport Layer Security and Secure Sockets Layer (TLS/SSL) in ADFS is mandatory.

Account partner cookie

The *account partner cookie* facilitates single sign-on. After interactive account partner membership discovery occurs, if the account partner cookie has a valid token, the cookie is written to the client. Further interactions use the information in this cookie rather than prompting the client for account partner membership information again. The account partner cookie is set as a result of the account partner discovery process.

The account partner cookie is a long-lived, persistent cookie. It is neither signed nor encrypted.

Sign-out cookie

The *sign-out cookie* facilitates sign-off. Whenever the Federation Service issues a token, the token's resource partner or target server is added to the sign-out cookie. When it receives a sign-off request, the Federation Service or Federation Service Proxy sends requests to each of the token target servers asking them to clean up any authentication artifacts, such as cached cookies, that the resource partner or Web server may have written to the client. In the case of a resource partner, it sends a cleanup request to any application Web servers that the client has used.

The sign-out cookie is always a session cookie. It is neither signed nor encrypted.

ADFS Operations

This section contains the following topics to assist the administrator in securely operating ADFS within the TOE:

- Reading the Log Files
- Adding an ADFS-enabled Application
- Adding a federation server proxy

Reading the Log Files

To monitor ADFS activities and troubleshoot ADFS problems, administrators should look at the event logs and debug logs generated by ADFS components. This section describes the following logging types:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- ADFS Event Logging
- ADFS Debug Logging
- Web Error Reporting

ADFS Event Logging

Administrators can configure event logging on federation servers, federation server proxies, and Web servers. ADFS events are logged in the Application event log and the Security event log.

> **Note:** Audit object access must be enabled at each of the federation servers for ADFS-related audits to appear in the Security log. This allows the Federation Service to log either success or failure errors. For more information about how to turn on auditing of object access, see Configuring Audit Policies in this document.

Procedures for configuring event logging on ADFS computers can be found in the **ADFS Configuration and Installation** sections of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Event logs are generally descriptive, intended to help you understand what is happening. However, if there are issues with ADFS functionality, the default events do not always provide the level of detail that is needed for effective troubleshooting. In cases like that, configure ADFS debug logging.

Event logging on the federation server

Servers that are running the Federation Service component of ADFS log ADFS Federation Service events in the Application event log. These events report information about the operation of the components of the local organization and partner organizations that are covered by a trust policy.

The following types of events are available and enabled by default in ADFS:

- **Error**: Information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **Information**: Information about a significant, successful operation.
- **Success audit**: Indicates an audited security event that when an audited access attempt is successful; for example, a successful logon attempt.
- **Detailed success**: A success audit event with detailed information about each token involved in the transaction, including claims information.
- **Warning**: Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Failure audit**: Indicates a security event that occurs when an audited access attempt fails; for example, an inbound token was not valid.
- **Detailed failure**: A failure audit event with detailed information about each token involved in the transaction, including claims information.

On federation servers, use the Windows interface to verify or change event logging levels. Procedures for verifying or changing the default events logged by ADFS can be found in the **Configuring Event Logging on the Federation Servers** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Event logging on the federation server proxy

Administrators can specify the level of events to be logged on a server that is running the Federation Service Proxy component. Event logging for a federation server proxy is set in the Web.config file. By default, this file is located in %SystemDrive%\ADFS\sts. The following logging types can be applied:

- **DetailedFailure:** A failure audit event with detailed information about each token involved in the transaction, including claims information.
- **DetailedSuccess:** A success audit event with detailed information about each token involved in the transaction, including claims information.
- **Error:** Information about a significant problem of which the user should be aware, usually involving a loss of functionality or data.
- **FailureAudit:** Indicates a security event that occurs when an audited access attempt fails; for example, authentication failed.
- **Info:** Information about a significant, successful operation.
- **SuccessAudit:** Indicates an audited security event that when an audited access attempt is successful; for example, a successful logon attempt.
- **Warning:** Indicates a problem that is not immediately significant, but that may signify conditions that could cause future issues.
- **Everything:** Enable all logging levels.

Procedures for specifying the events logged by the Federation Service Proxy can be found in the **Configuring Event Logging on the Federation Server Proxy** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Note: To reduce the number of events generated by ADFS, return this value to a lesser value after reaching a problem resolution following any troubleshooting steps.

Event logging on the Web Server

Events logged on Web servers that are running an ADFS Web Agent are configured according to the application type that the agent supports. Event logging is configured differently for Windows NT token-based applications and claims-aware applications. Procedures for configuring this type of logging can be found in the **Configuring Event Logging on the Web Server** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

ADFS Debug Logging

ADFS provides several levels of debug information that are available for troubleshooting ADFS problems. Debug logging levels can be configured on federation servers, federation proxy servers, and Web servers that are running ADFS Web Agents.

Note: Debug logging consumes space and resources on the computer. Enabling debug logging is recommended only for troubleshooting a problem and there is a need for more information than is provided in the event logs. Otherwise, do not enable debug logging.

The debug log file is located in %SystemDrive%\ADFS\logs.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Debug logging on the federation server or federation server proxy

If debug logging is enabled on a federation server or federation server proxy, the log filename in the C:\ADFS\logs folder has the following format:

adfsyyyymmdd-hhmmss.log

In the name of the file, the number following "adfs" represents the date of the log and the number following the dash (-) represents the beginning time of the log.

Depending on the level of debug logging enabled, the following tags are displayed in debug logs:

- **[INFO]** - Displays information about events, such as redirects with protocol Uniform Resource Locators (URLs), token validations, or claim mappings.
- **[VERBOSE]** - Displays information about events, such as sign-in requests, responses, token contents, Web method calls, and security identifier (SID) information.
- **[ERROR]** - Displays events for significant problems in the debug log.
- **[WARNING]** - Displays events, which are not necessarily significant but that may cause future problems.
- **[EVENTLOG]** - Displays all ADFS events.

Although all information in the log file could be useful, an administrator can look at the lines that are tagged **[ERROR]** and **[WARNING]** first to quickly assess the problem.

On federation servers, use the Windows interface to enable debug logging and set levels to increase the detail of feedback in the logs. Procedures for doing this can be found in the **Configuring Debug Logging on the Federation Servers** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Note: The procedures for enabling debug logging on a federation server proxy are the same as the procedures for enabling debug logging on a federation server.

Debug logging on the Web Server

Debug logging can be enabled for the Web server components described here.

- The ADFS Web Agent running on ADFS Web servers has two components:
  - ADFS Token Authentication service (ifssvc.exe), which validates incoming tokens and cookies. Debug logging creates ifssvc.log in the C:\ADFS\Logs folder.
  - ADFS Web Agent Internet Server Application Programming Interface (ISAPI) extension (ifsext.dll), which handles the protocols that are used by ADFS to authenticate requests; and the ADFS Web Agent ISAPI filter (ifsfilt.dll), which assists the extension and enables user name logging in the Internet Information Services (IIS) log files. Debug logging creates the ifsext_StsAppPool1.log and ifsfilt_StsAppPool1.log, respectively in the C:\ADFS\Logs folder.
- In addition, the ADFS Web Agent authentication package (ifsAp.dll) is used by Windows NT token-based applications for generating tokens when Service-for-User (S4U) is not available. Debug logging creates ifsap.log in the C:\ADFS\Logs folder.

Administrators can enable debug logging for each of these components by modifying the registry on the Web server. Procedures for doing this can be found in the **Configuring Debug Logging on the Web Server** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Web Error Reporting

CustomErrors is an ASP.NET element that provides information about custom error messages for an ASP.NET application. Setting the customErrors mode attribute to "Off" in the Web.config file on the federation servers specifies that custom errors are disabled. This results in better ADFS Web error reporting in the client's Web browser. For more information, see the **Configuring Web Error Reporting on the Federation Servers** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Adding an ADFS-enabled Application

When it's time to add another ADFS-enabled application to the TOE, administrators should consult the appropriate **ADFS Installation and Configuration** topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* for procedures required for configuring a new application. The topic chosen is dependent upon which scenario is in use: Federated Web SSO or Web SSO.

Adding an application in a Federated Web SSO scenario

To add an application in a Federated Web SSO scenario, the administrator must perform the tasks listed in table below and outlined in the **ADFS Installation and Configuration: Federated Web SSO Scenario** section of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Tasks and their associated topics and procedures in the configuration guide for adding an application in a Federated Web SSO scenario

Task	Topic in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*
Install and configure the application on the Web server	Topic: **Installing and Configuring a Claims-aware Application,** or **Installing and Configuring a Windows NT Token-based Application**
Configure the federation service 1. Create a group claim for the application 2. If the application is a Windows NT token-based application, add a resource group to the application claim 3. Add a group claim extraction to the account store for the application 4. Add the application 5. Enable the application claim	Topic: **Configuring the Federation Service** Procedures: 1. Create a group claim for the claims-aware application, **or** create a group claim for the Windows NT token-based application 2. For a Windows NT token-based application only, add a resource group to the Windows NT token-based application claim 3. Add a group claim extraction to the account store for the claims-aware application, **or** add a group claim extraction to the account store for the Windows NT token-based application 4. Add a Windows NT token-based application, **or** Add a claims-aware application 5. Enable the TokenApp Claim, **or** Enable the ClaimApp Claim.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Adding an application in a Web SSO scenario

To add an application in a Web SSO scenario, the administrator must perform the tasks listed in the table below and outlined in the **ADFS Installation and Configuration: Web SSO Scenario** section of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Tasks and their associated topics and procedures in the configuration guide for adding an application in a Federated Web SSO scenario

Task	Topic in the Window Server 2003 with SP2 Security Configuration Guide, Version 3.0
Install and configure the application on the Web server	Topic: **Installing and Configuring a Claims-aware Application**, or **Installing and Configuring a Windows NT Token-based Application**
Configure the federation service on the resource federation server: 1. Create a group claim for application 2. If the application is a Windows NT token-based application, add a resource group to the application claim 3. Add the application 4. Enable the application claim 5. Create an incoming group claim mapping for the application	Topic: **Resource Partner: Configuring the Federation Service on the Resource Federation Server** Procedures: 1. Create a group claim for the claims-aware application, **or** create a group claim for the Windows NT token-based application 2. For a Windows NT token-based application only, add a resource group to the Windows NT token-based application claim 3. Add the claims-aware application, **or** add a Windows NT token-based application 4. Enable the <AccountDomain> ClaimApp Claim for both claims-aware applications, **or** enable the <AccountDomain> TokenApp Claim 5. Create an incoming group claim mapping for the claims-aware application, **or** create an incoming group claim mapping for the Windows NT token-based application
Configure the federation service on the account federation server 1. Create a group claim for the application 2. Map a global group to the group claim 3. Create an outgoing group claim mapping	Topic: **Account Partner: Configuring the Federation Service on the Account Federation Server** Procedures: 1. Create a group claim for the claims-aware applications, **or** create a group claim for the token-based application 2. Map a global group to the group claim for the claims-aware application, **or** map a global group to the group claim for the token-based application 3. Create an outgoing group claim mapping for the claims-aware application, **or** create an outgoing group claim mapping for the token-based application

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Adding a federation server proxy

When there is an existing Active Directory Federation Services (ADFS) deployment and a need to add a new federation server proxy, the administrator must configure the server as an application server, install and configure certificates, and then install the Federation Server Proxy component of ADFS. Adding an additional federation server proxy creates an environment that is sometimes described as a "farm" because it contains multiple instances of a server component.

Farmed sets of federation server proxies must share the certificate public key with the Federation Service that they protect. However, the administrator must export the public key from each federation server proxy and add this key to the shared trust policy of the Federation Service as a Federation Service Proxy (FSP) verification certificate.

During installation, configure the federation server proxy with the Domain Name System (DNS) host name of the protected Federation Service. This name is added automatically to create the Federation Service URL, which the federation service proxy uses to communicate with the Federation Service.

The following is needed in order to perform the procedures for adding a federation server proxy:

- An installed Secure Sockets Layer (SSL) server authentication certificate.
- An existing Federation Service.
- The DNS host name of the Federation Service that this federation server proxy will protect.
- An installed client authentication certificate for the Federation Service Proxy.

To complete this task, consult the topics in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* as indicated in the table below.

Tasks and their associated topics and procedures in the configuration guide for adding a federation server proxy

Task	Topic in the Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0
Install prerequisite applications	Topic: **ADFS Installation Preparation**
Install the Federation Service Proxy on an addition federation server proxy	Topic: **Installing the Federation Service Proxy**
Export the public key portion of a client authentication certificate	Topic: **Exporting the Client Authentication Certificate Public Key**
Add a Federation Service Proxy (FSP) certificate to the trust policy	Topic: **Configuring the Federation Service** Procedure: Add the Federation Service Proxy client authentication certificate to the federation server trust policy
Configure event logging on the federation server proxy	Topic: **Configuring Event Logging on the Federation Server Proxy**

Administering Windows Server Update Services

Microsoft® Windows™ Server Update Services (WSUS) 3.0 is included in the TOE to support the deployment of Microsoft product updates to Windows Server 2003 and Windows XP operating systems. By using WSUS 3.0, administrators can fully manage the distribution of updates to all clients. Within the TOE, the only updates that are allowed to be approved for installation on computers are those listed in Table 3.4 of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* (this document) and Table 3.3 of the *Windows XP Professional with SP2 Security Configuration Guide, Version 3.0*. All computers within the TOE, once installed and configured, will include all of the updates shown under the **Required Security Update** column of Tables 3.3 and 3.4 in the respective Security

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Configuration Guides. Therefore, the only remaining updates that may be approved for installation WSUS 3.0 clients within the TOE are those shown under the **Recommended Security Update** column of Tables 3.3 and 3.4 in the respective Security Configuration Guides.

WSUS 3.0 administrators can specify the types of updates clients can download, create target groups of computers to receive updates, and determine which computers require updates before deployment. Administrators can approve updates for deployment automatically, uninstall updates, and generate reports to monitor update activity. The procedures used to manage and approve updates for installation on WSUS 3.0 clients within the TOE, are provided in this document.

WSUS 3.0 uses the Windows Installer Service to deploy updates and provide a standard format for component management. The Windows Installer Service supports advertisement of applications and features according to the operating system settings. It can install multiple patches with a single transaction that integrates installation progress, rollback, and reboots. It can apply patches in a constant order regardless of the order that the patches are provided to the system. Patches installed with the Windows Installer Service can be uninstalled in any order to leave the state of the product the same as if the patch was never installed. Patching using Windows Installer Service only updates files affected by the patch. Accounts with administrator privileges can use Windows Installer Service functions to query and inventory product, feature, component and patch information and to read, edit and replace installer source lists for network, URL and media sources. Administrators can enumerate across user and install contexts and manage source lists from an external process.

Security Functionality

The following security functionality is supported for the administration of WSUS:

- Update server logging, where the TOE generates a log entry for update downloads and WSUS configuration settings events with at least the update status, computer status and synchronization status.
- Management of WSUS configuration settings, including time and security settings, where the ability to modify WSUS configuration settings is restricted to authorized administrators.

Logging

WSUS 3.0 creates a log recording of its activities which contains the following information:

- **Download status** – The log contains records of individual computer's activities with respect to particular downloads. Whenever a download is accessed by a computer, an entry is added to the log.
- **Configuration settings** – The log contains a record of the configurations settings for the WSUS.

The authorized administrator can view the log file and correlate such information as:

- **Computer status** – Administrators can assess the status of client computers with respect to the status of updates on those computers-for example, a summary of updates that have been installed or are needed for a particular computer.
- **Update status** - Administrators can view or print a summary of compliance information for a specific update, including the update properties and cumulative status for each computer group.
- **Synchronization (or download) status** - Administrators can monitor synchronization activity (i.e., client communications with the WSUS) and status for a given time period, and view the latest updates that have been downloaded.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Management

A WSUS 3.0 administrator has the ability to approve or unapproved updates for installation. If the administrator approves an updates, the update can then be either pushed or pulled from the server. In a pull operation, the administrator can let client machines poll the server looking for new updates. In the push operation, WSUS server downloads updates and pushes them to the Auto Update Client on each client computer within the TOE. The client then installs the updates. The administrator can configure the server to require all client machines to perform an immediate update. The administrator also has the ability to set a deadline by which time all clients must download an update (i.e., perform a pull operation) or the server will push the update. Specific WSUS security administration includes:

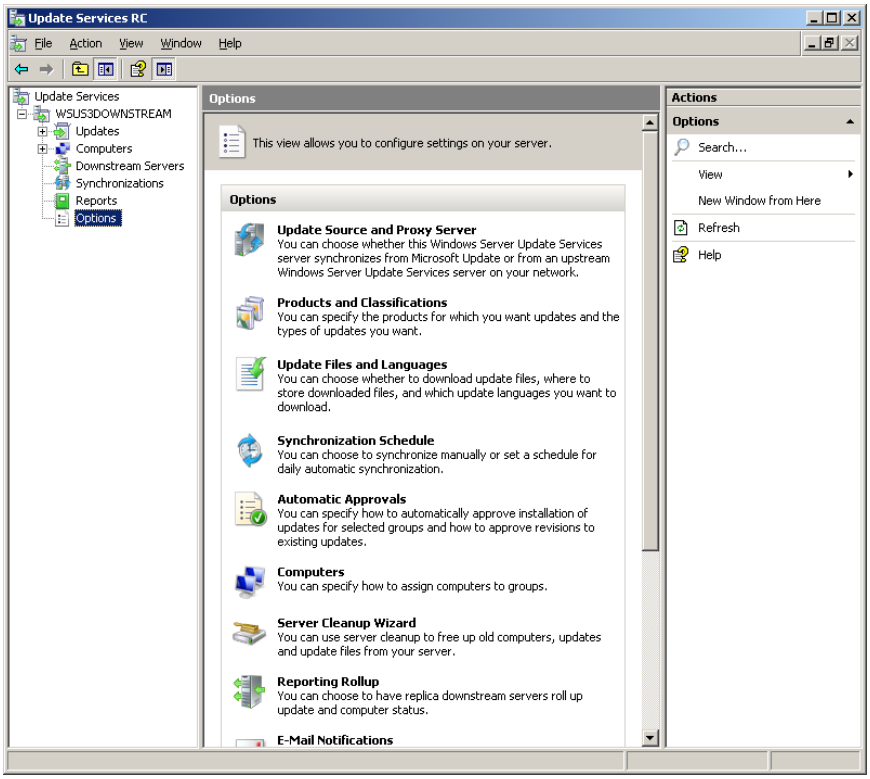
- **WSUS Update Installation**. WSUS 3.0 allows the ability to install administrator-specified updates from the list of available updates on specified computers.
- **WSUS Update Advertisement**. WSUS 3.0 allows the ability to advertise the availability of software updates imported by the authorized administrator to computers within the TOE.
- **WSUS Update Import**. WSUS 3.0 restricts the ability to import software updates for distribution within the TOE to only authorized administrators.
- **WSUS Update Distribution Approval**. WSUS 3.0 restricts the ability to approve software updates for distribution within the TOE to only authorized administrators.
- **Application of WSUS Updates**. A WSUS 3.0 server, external to the TOE, polls the Microsoft Update Web site looking for new updates. Once downloaded, these updates are then exported onto removable media and then imported to a WSUS 3.0 server within the TOE where administrator-approved updates are then pushed to the client machines for installation.
- **WSUS Update Deadlines**. WSUS 3.0 restricts the ability to enforce an update deadline for updates to be installed to only authorized administrators and enforces the rule that update deadlines can be immediately applied.

Access the WSUS 3.0 administration interface

Individuals authorized to administer WSUS 3.0 must be members of the local Administrators group or the WSUS Administrators security group on the computer on which WSUS is installed in order to use all the features of the WSUS 3.0 administration interface. To open the WSUS 3.0 administration interface, click **Start**, point to **Administrative Tools**, and select **Windows Server Update Services 3.0**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Managing Windows Server Update Services

This section explains how to set up and run synchronizations, manage computers and computer groups, manage updates, and run in replica mode.

WSUS 3.0 Synchronizations

The specific procedures for synchronizing a WSUS 3.0 server within the TOE vary, depending on whether the WSUS 3.0 server is the only WSUS server in the architecture, an upstream server in a hierarchical WSUS 3.0 architecture, or a downstream server in a hierarchical WSUS 3.0 architecture within the TOE. Synchronizing an upstream or a standalone WSUS 3.0 server within the TOE requires that the updates be imported from a WSUS 3.0 server that is outside the TOE. Synchronizing a downstream WSUS 3.0 server within the TOE involves contacting an upstream server for updates and downloading the new updates from the upstream server across the local network.

Synchronizing updates on upstream or single WSUS server architectures

Since the TOE is disconnected from the Internet, upstream or single WSUS 3.0 server architectures cannot contact the Microsoft Update Web site in order to synchronize and obtain updates. It is therefore necessary to export updates and metadata from a WSUS 3.0 server that is external to the TOE and has access to the Microsoft Update Web site via the Internet. The external WSUS 3.0 server is synchronized with the Microsoft Update Web site in order to download the updates that are to be distributed to computers within the TOE. Once exported from the external WSUS 3.0 server, the updates and corresponding metadata are imported to WSUS 3.0 servers within the TOE and their distribution to WSUS client computers within the TOE can be managed.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The three basic steps to exporting and then importing updates are listed below. Detailed procedures for each of these steps are provided in the *Window Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

1. Make sure that the options for express installation files and update languages on the external WSUS 3.0 server are compatible with the settings on the WSUS 3.0 servers within the TOE. This ensures that the proper updates are collected for distribution.
2. Backup the updates from the file system of the external WSUS server and then restore those updates to the file system of the WSUS 3.0 servers within the TOE. This would be to the upstream or single WSUS 3.0 servers within the TOE. Downstream WSUS 3.0 servers within the TOE will obtain their updates from the upstream WSUS 3.0 server.
3. Export update metadata from the database of the external WSUS 3.0 server, and import it into the database of the upstream or single WSUS 3.0 servers within the TOE.

Synchronizing updates on downstream WSUS servers

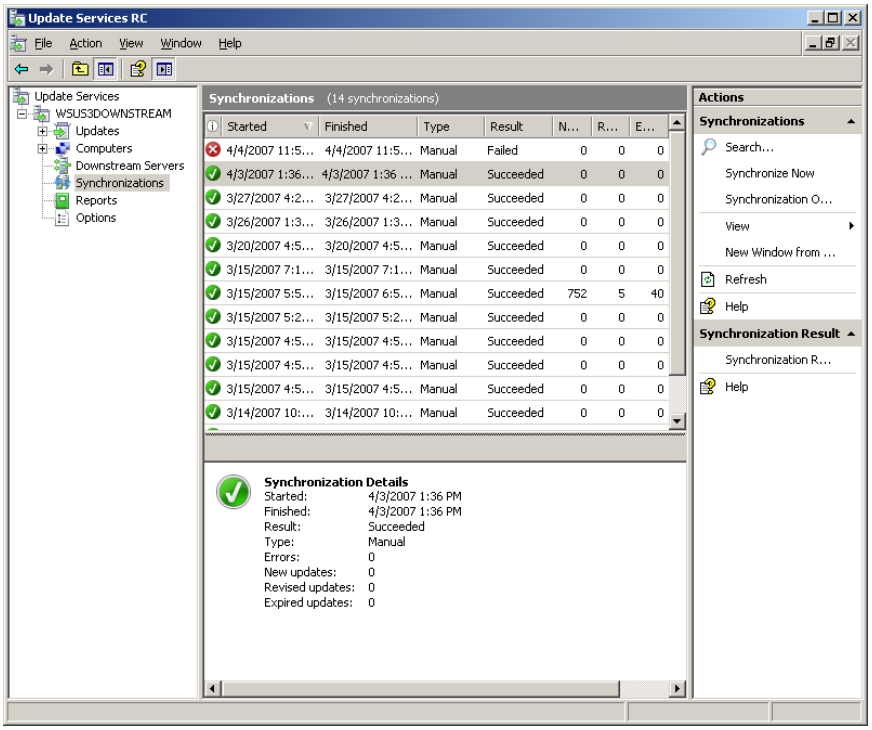
Synchronizing a downstream server involves contacting an upstream WSUS 3.0 server within the TOE to check for and download new updates. The downstream WSUS server determines if any new updates have been made available since the last time it was synchronized. If this is the first time synchronizing the WSUS server, all of the metadata for updates in the product categories and classifications that administrators have selected are synchronized to the downstream WSUS server. Procedures for initially setting up and synchronizing a downstream WSUS 3.0 server within the TOE are provided in *Window Server 2003 with SP2 Security Configuration Guide, Version 3.0*. Follow the procedure below to manually synchronize a downstream WSUS 3.0 server.

Note: The first synchronization on a WSUS server will generally take a long time. Administrators will not be able to make changes to the server's update filters (products, classifications, languages) while the server is being synchronized.

1. In the Update Services interface, right-click the **Synchronizations** node and select **Synchronize Now**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



2. After the synchronization finishes, click **Updates** in the tree view for this server to review and manage the list of updates.

Managing Updates

Updates are used for patching or providing a full file replacement for software that is installed on a computer. Every update that is available on Microsoft Update is made up of two components:

- **Metadata** provides information about the update. For example, metadata supplies information for the properties of an update, thus describing what the update is useful for. Metadata also includes end-user license agreements (EULAs). The metadata package downloaded for an update is typically much smaller than the actual update file package.
- **Update files** are the actual files required to install an update on a computer.

Managing Updates with WSUS

Administrators will be setting up and running synchronizations, adding computers and computer groups, and deploying updates on a regular basis. The following gives examples of general tasks to undertake in updating computers with WSUS 3.0.

1. Determine an overall update management plan based on network topology and bandwidth, company needs, and organizational structure. Considerations might include the following:
   - Whether to set up a hierarchy of WSUS servers, and how the hierarchy should be structured.
   - What computer groups to create, and how to assign computers to them (server-side or client-side targeting).
   - Whether updates should be synchronized automatically, and at what time.
2. Set synchronization options, such as update source, product and update classification, language, connection settings, storage location, and synchronization schedule.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. Get the updates and associated metadata on the WSUS server through data import from an external WSUS server or synchronization with an upstream WSUS server.
4. Approve or decline updates. Administrators have the option of allowing users to install the updates themselves (if they are local administrators on their client computers).
5. Configure automatic approvals. Administrators can also configure whether to enable automatic approval of revisions to existing updates or approve revisions manually. If administrators choose to approve manually, then the WSUS server will continue using the older version until the new version is manually approved.
6. Check the status of updates. Administrators can view update status, print a status report, or configure e-mail for regular status reports.

A *product* is a specific edition of an operating system or application, for example Microsoft Windows Server 2003. A *product family* is the base operating system or application from which the individual products are derived. An example of a product family is Microsoft Windows, of which Microsoft Windows Server 2003 is a member. Administrators can select the products or product families for which to synchronize updates with the server. Administrators can specify a product family or individual products within the family. Selecting any product or product family will get updates for current and future versions of the product.

Update Classifications

Update classifications represent the type of update. For any given product or product family, updates could be available among multiple classifications (for example, Windows XP family Critical Updates and Security Updates). The following table lists update classifications.

Update Classification	Description
Critical Updates	Broadly released fixes for specific problems addressing critical, non-security related bugs.
Definition Updates	Updates to virus or other definition files.
Development Kits	Software to aid the writing of new applications
Drivers	Software components designed to support new hardware
Feature Packs	New feature releases, usually rolled into products at the next release
Security Updates	Broadly released fixes for specific products, addressing security issues
Service Packs	Cumulative sets of all hotfixes, security updates, critical updates, and updates created since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.
Tools	Utilities or features that aid in accomplishing a task or set of tasks
Update Rollups	Cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a specific component, such as Internet Information Services (IIS).
Updates	Broadly released fixes for specific problems addressing non-critical, non-security related bugs

Viewing the Updates

From the **Updates** node of the Update Services interface, administrators can do the following:

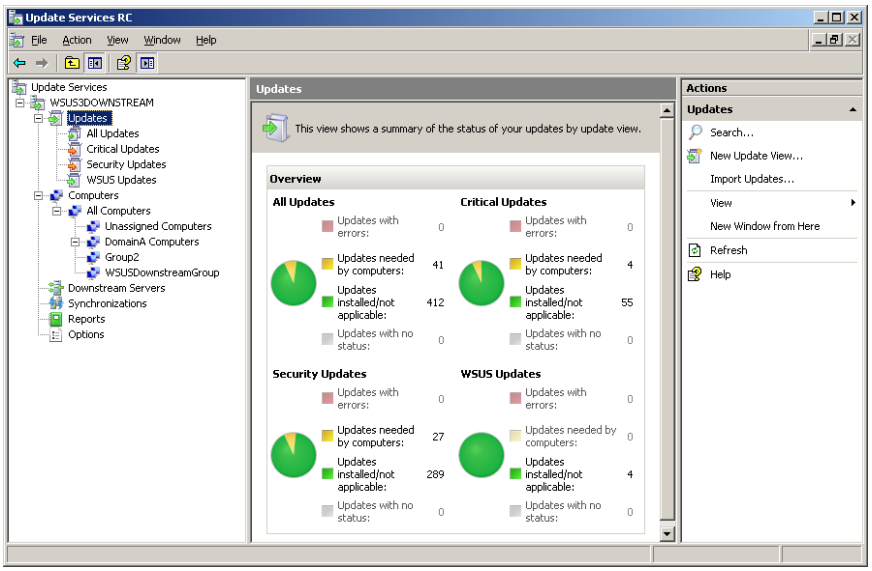
Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **View updates**. The update overview displays updates that have been synchronized from the update source to the WSUS server and are available for approval.
- **Filter updates**. In the default view, administrators can filter updates by approval status and installation status. The default setting is for unapproved updates that are needed by some clients, or which have had install failures on some clients. Administrators can change this view by changing the approval status and install status filters, then clicking **Refresh** from the Actions pane.
- **Create new update views**. In the Actions pane, click on **New Update View**. Administrators can filter updates by classification, product, the group for which they have been approved, and synchronization date. Administrators can sort the list by clicking the appropriate column heading in the title bar.
- **Search for updates**. Administrators can search for an individual update or set of updates by title, description, Knowledge Base article, or the Microsoft Security Response Center number for the update.
- **View details, status, and revision history for each update.**
- **Approve updates.**
- **Decline updates.**

To view update summary

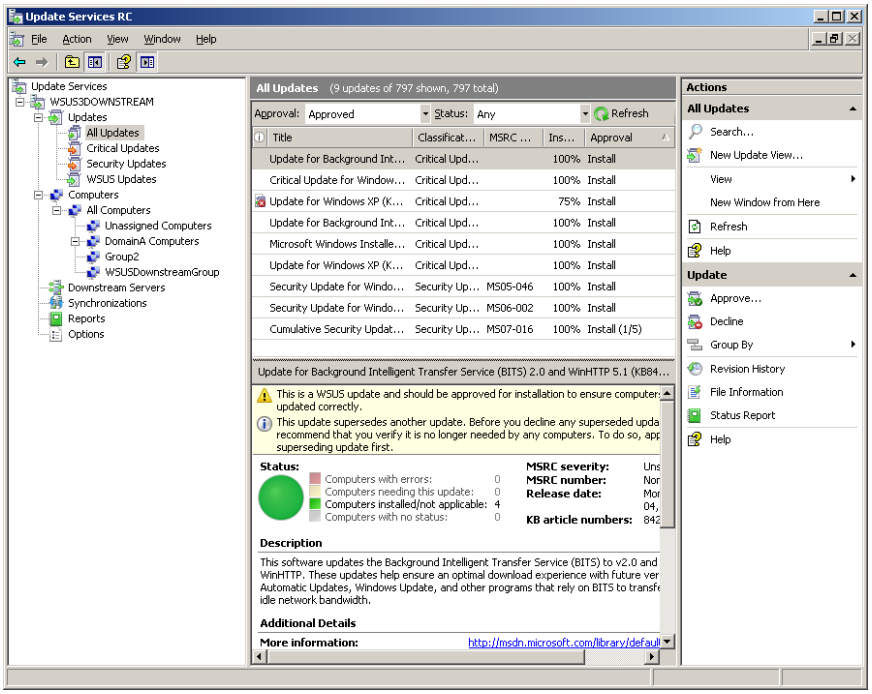
In the Update Services interface, double-click the **Updates** node.



To view detailed updates

In the Update Services interface, expand the **Updates** node, and double-click on **All Updates**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

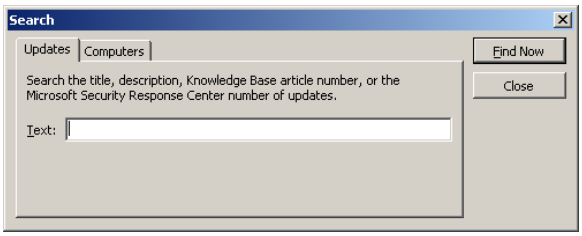


Notes:

- By default, updates are displayed with their title, classification, installed/not applicable percentage, and approval status. To display more or different update properties, right-click the column heading bar and select the appropriate columns.
- To sort by different criteria, such as download status, title, classification, release date, or approval date, click the appropriate column heading.

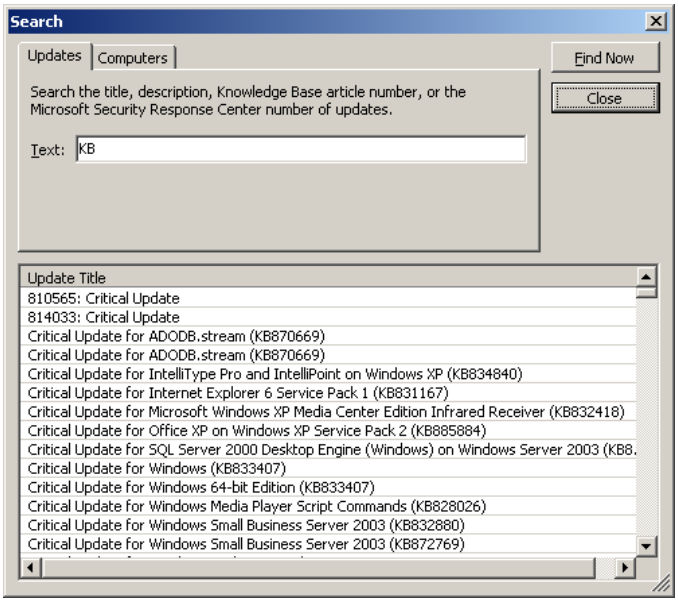
To search for a particular update

1. Select either the **Updates** node (or any node under it).
2. In the Actions pane, click **Search** to bring up the **Search** window.

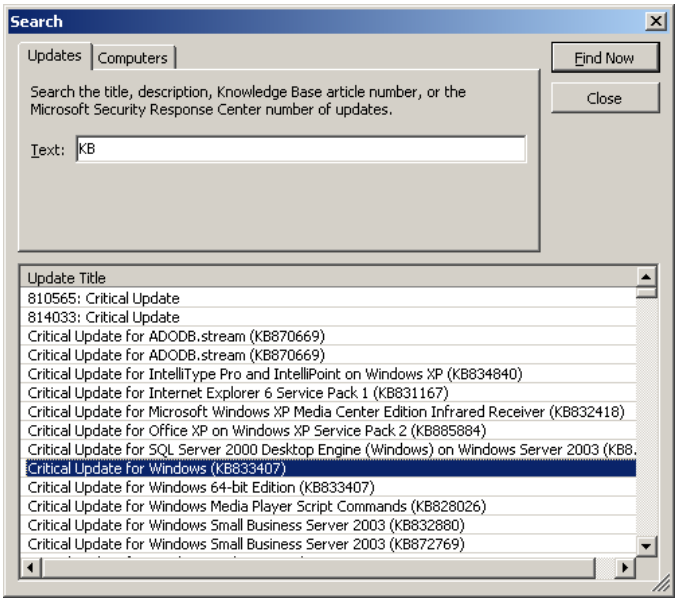


3. In the **Search** window, enter the title, description, or Knowledge Base (KB) article number (as known) into the **Text** box of the Updates tab and click **Find Now** to commence. Once search is completed, all updates with the entered criteria will be listed.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

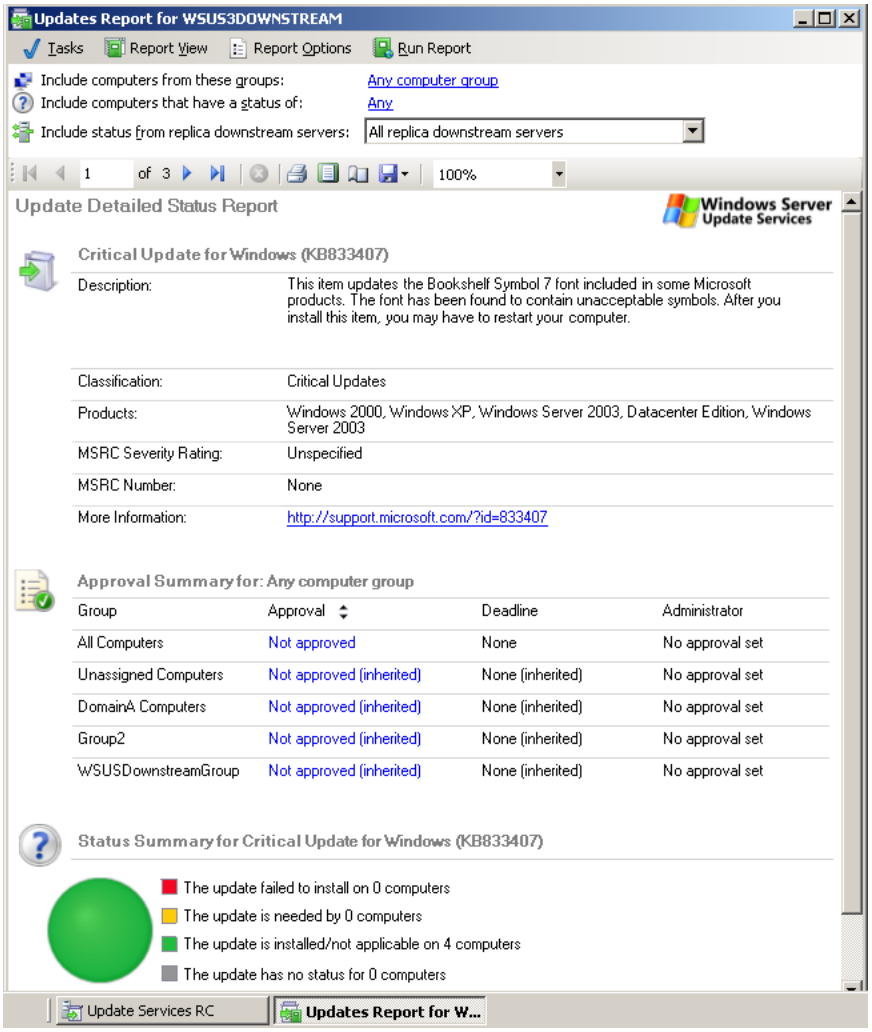


4. To view the details, double-click on one to review.



5. A detailed report will display.

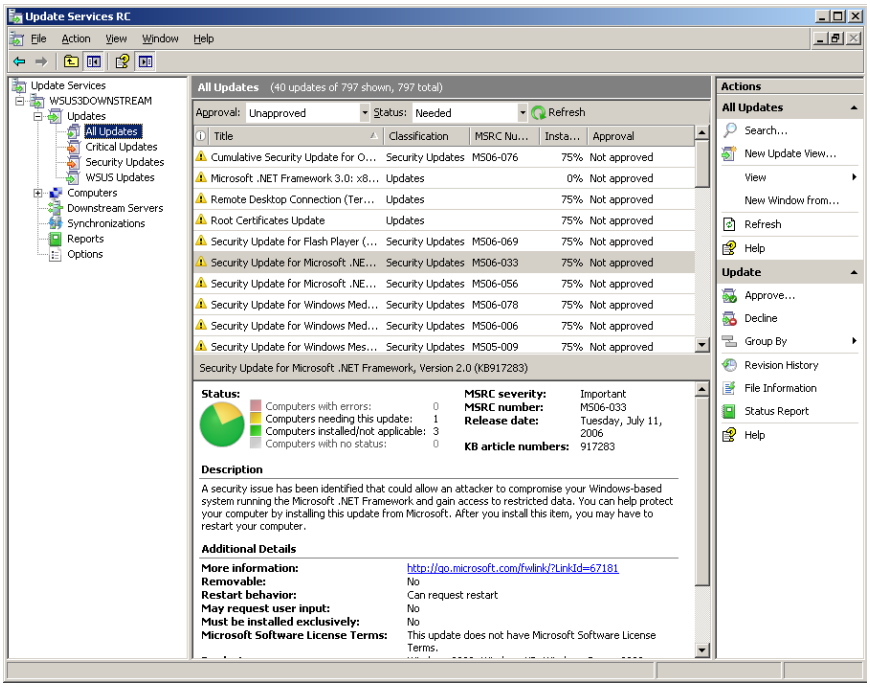
Copyright © 2008 Microsoft Corporation.
All rights reserved.



To filter the list of updates displayed on the Updates page

1. In the Update Services interface, expand the **Updates** node and double click **All Updates**.
2. In the center pane, next to **Approval:** scroll down and select option desired such as **Unapproved**.
3. In the center pane next to **Status:** scroll down and select option desired such as **Needed**.
4. In the center pane, click on the **Refresh** button to display all unapproved/needed updates pending action.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. Double-click on each update listed to review its **Update Detailed Status Report**.

Warning: This procedure can be performed on only one update at a time. If multiple updates are selected, only the first update in the list will be displayed in the properties pane.

To view the properties for an update

There are two options for viewing the properties of an update.

Option A – highlight the desired update and review the Status summary listed in the bottom half of the center pane for the highlighted update. Lower pane Status options visible include:

- The title bar displays the title of the update, for example, **Security Update for Windows Media Player 9 (KB911565)**.
- The **Status** section displays the installation status of the update (the computers on which it needs to be installed, computers on which it was installed with errors, computers on which it has been installed or is not applicable, and computers that have not reported status for the update), as well as general information (KB and MSRC numbers release date, etc.).
- The **Description** section displays a brief description of the update.
- The **Additional Details** section displays the following information:
  - the installation behavior of the update (whether or not it is removable, requests a restart, requires user input, or must be installed exclusively)
  - whether or not the update has Microsoft Software License Terms
  - the products to which the update applies
  - the updates that supersede this update
  - the updates that are superseded by this update
  - the languages supported by the update

Copyright © 2008 Microsoft Corporation.
All rights reserved.

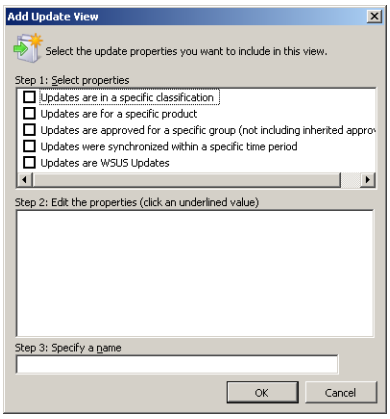
- the update ID

Option B [reflected separately under Reports] – double-click to bring up the separate, Update Detailed Status Report that includes:

- The update title section that displays the following information:
  - Description
  - Classification
  - Products affected
  - MSRC severity rating and number
- The **Approval Summary for:** <listing by selection of group(s)> that displays Group, Approval, Deadline and Administrator action(s) by listed group(s)
- The **Status Summary** section for the specifically identified update displays statistics as to whether the update failed to install on computers; is needed by computers; is installed/not applicable on computers; no status for computers
- **Computer Detailed Status Report** (page 2) lists computer name, approval status and installation status
- **Report Options** (page 3) lists report type, classifications, products, computer groups, status, downstream servers, report data collected day/time, and server used for reporting data.

To create a new update view

1. In the Update Services interface, expand the **Updates** node and double-click **All Updates** to list.
2. In the **Actions** pane on the right side, double-click **New Update View…** to bring up the **Add Update View** window.



3. Under Step 1: Select properties, select the update properties to be included in new view, such as:

- Select **Updates are in a specific classification** to filter on updates belonging to one or more update classifications, or
  - Select **Updates are for a specific product** to filter on updates for one or more products or product families, or
  - Select **Updates are approved for a specific group** to filter on updates approved for one or more computer groups, or
  - Select **Updates were synchronized within a specific time period** to filter on updates synchronized at a specific time, or

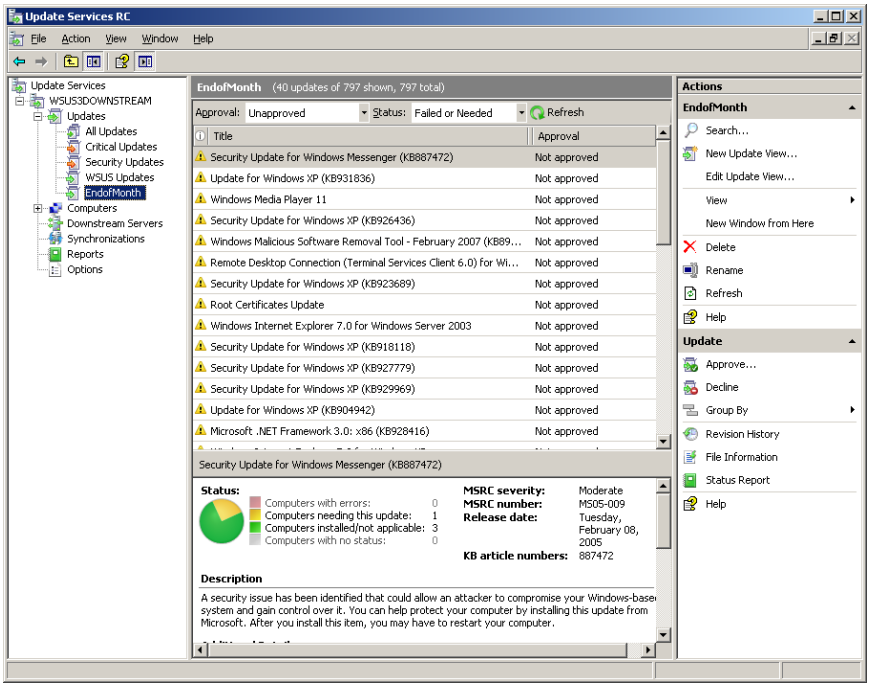
Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Select **Updates are WSUS updates** to filter on WSUS updates.

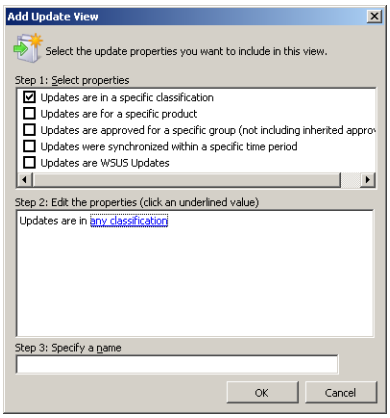
4. Under Step 2: Edit the properties (click an underlined value), complete actions desired by update selection, as follows.

5. Under Step 3: Specify a name, enter a name in the box for each new update view created and click OK to save/exit the new Update category. The new view will appear in the tree view pane under Updates. It will be displayed, like the standard views, in the center pane when selecting it.



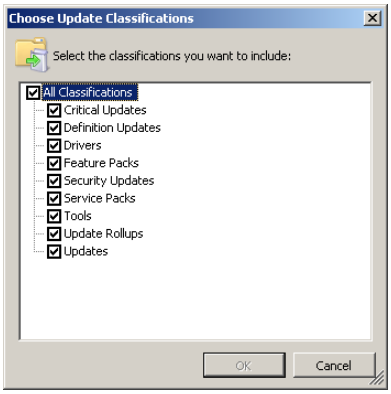
Modify the Updates are in a specific classification option

1. If in the Step 1: Select properties box, the **Updates are in a specific classification** box is checked, **Step 2: Edit the properties (click an underlined value)** option is displayed only as **Updates are in any classification**.



2. To view, click on **any classification** to bring up the Choose Update Classifications window and make any changes desired, click on OK to save/exit.

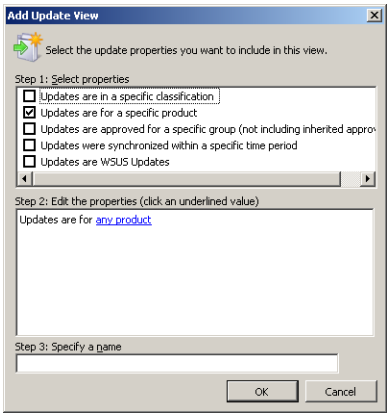
Copyright © 2008 Microsoft Corporation.
All rights reserved.



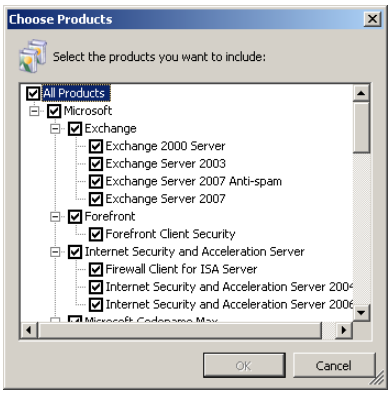
Note: This option will not display anything in **Step 3: Specify a name** field of the **Add Update View** window.

Modify the Updates are for a specific product option

1. If in the Step 1: Select properties box, the **Updates are for a specific product** box is checked, **Step 2: Edit the properties (click an underlined value)** option is displayed only as **Updates are for any product**.



2. To view, click on **any product** to bring up the Choose Products window and make any changes desired, click on OK to save/exit.



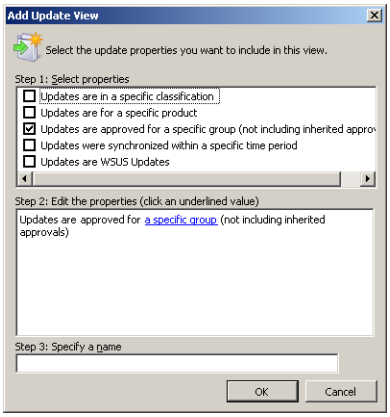
Note: This option will not display anything in **Step 3: Specify a name** field of the **Add Update View** window.

Copyright © 2008 Microsoft Corporation.

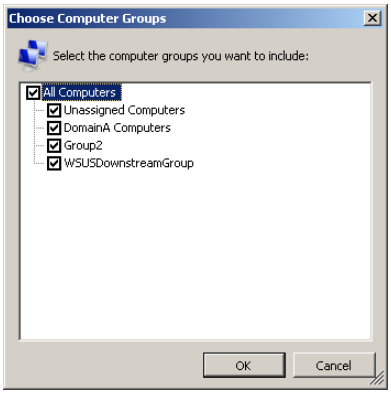
All rights reserved.

Modify the Updates are approved for a specific group (not including inherited approvals) option

1. If the Step 1: Select properties box selects Updates are approved for a specific group (not including inherited approvals) is checked, Step 2: Edit the properties (click an underlined value) option is displayed only as Updates are approved for a specific group (not including inherited approvals).



2. To view, click on a **specific group** to bring up the Choose Computer Groups window and make any changes desired by checking the appropriate box(es) and clicking OK to save/exit.



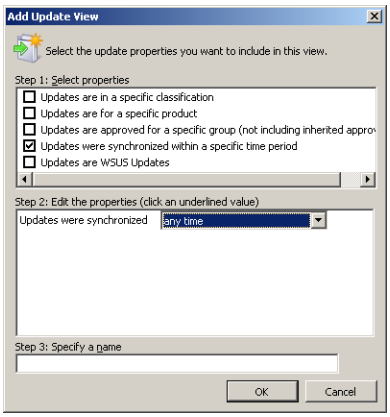
Note: This option will not display anything in **Step 3: Specify a name** field of the **Add Update View** window.

Modify the Updates were synchronized within a specific time period option

1. If the **Step 1: Select properties** box selects **Updates are WSUS Updates** is checked, **Step 2: Edit the properties (click an underlined value)** option is displayed only as **Updates were synchronized** and contains a drop down menu where either **any time, within the last week, within the last month, within the last two months** option can be selected, depending on desire.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

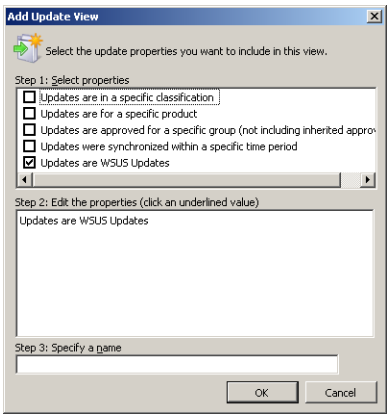


2. Click **OK** after option selected to save/exit.

Note: This option will not display anything in **Step 3: Specify a name** field of the **Add Update View** window.

Modify the Updates are WSUS Updates option

1. If the Step 1: Select properties box selects Updates are WSUS Updates is checked, Step 2: Edit the properties (click an underlined value) option is displayed only as Updates are WSUS Updates.



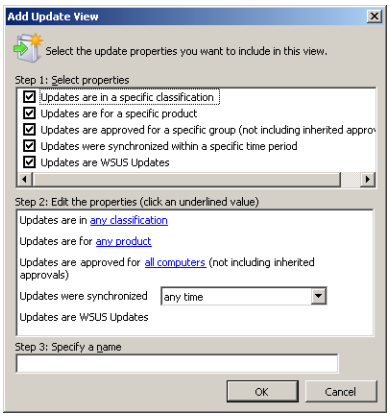
2. Click OK to save/exit.

Note: This option will not display anything in **Step 3: Specify a name** field of the **Add Update View** window.

All Add Update View option

1. If the Step 1: Select properties box selects (checked) all:
   - **Updates are in a specific classification**, and
   - **Updates are for a specific product**, and
   - **Updates are approved for a specific group (not including inherited approvals)** , and
   - **Updates were synchronized within a specific time period**, and
   - **Updates are WSUS Updates** are checked

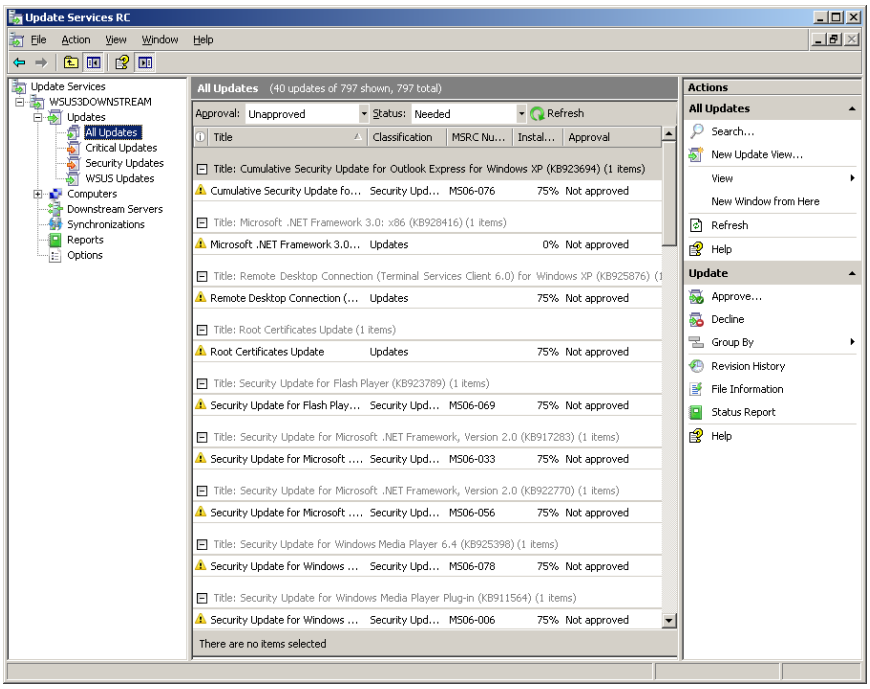
Copyright © 2008 Microsoft Corporation.
All rights reserved.



2. The resultant values in Step 2: Edit the properties (click an underlined value) must be completed individually.
3. Click OK to save/exit.

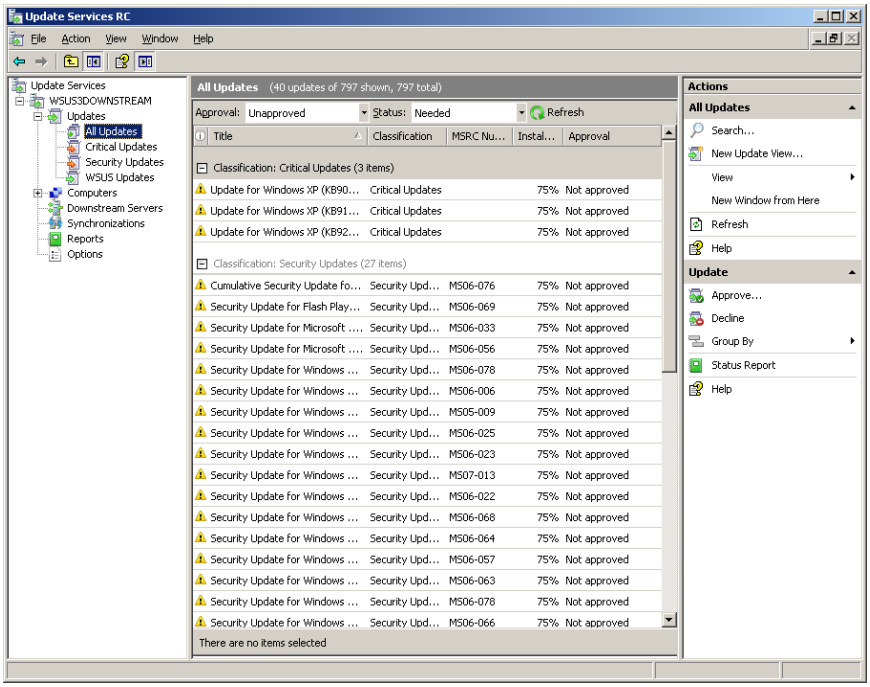
Sorting the update list

1. In the Update Services interface, expand Updates and click All Updates to obtain the list of all updates.
2. Right-click on an update in the center list to bring up drop-down window that reflects Approve, Decline, Group By, Status Report and Help. Scroll down and select Group By.
3. Scroll over and select option desired as either:
   - **Title** to display the available update by title:

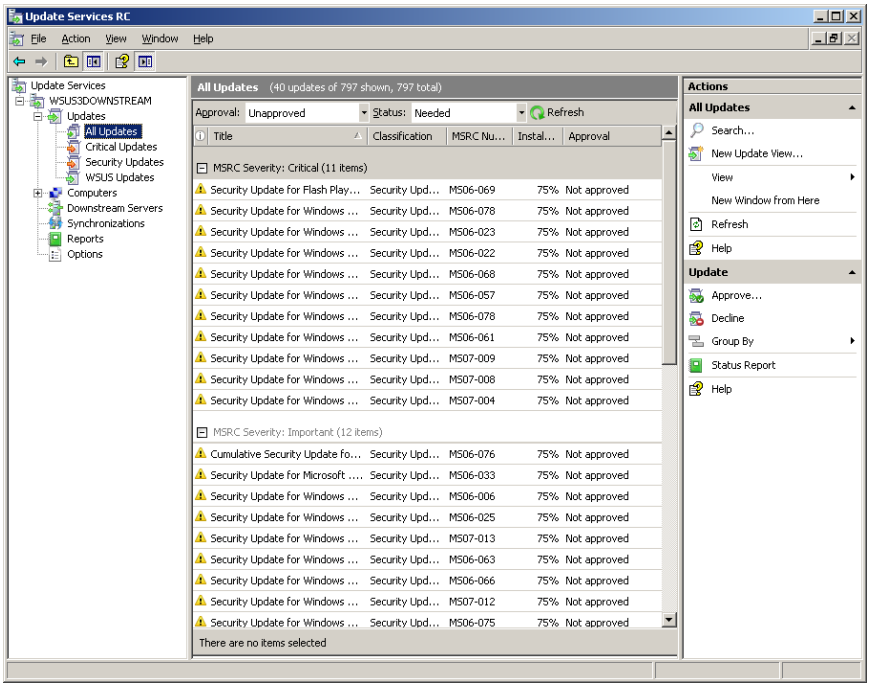


   - **Classification** to list the updates by Classification (i.e., Critical, Security, Update Rollups, Updates):

Copyright © 2008 Microsoft Corporation.
All rights reserved.

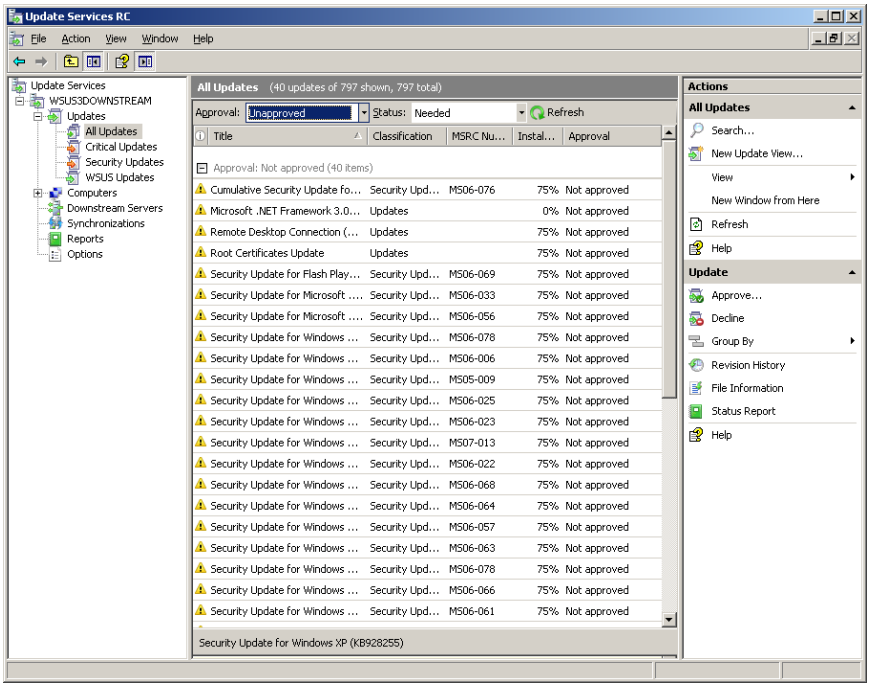


- **MSRC Severity** to list the updates by MSRC Severity (i.e., Critical, Important, Low, Moderate, Unspecified):

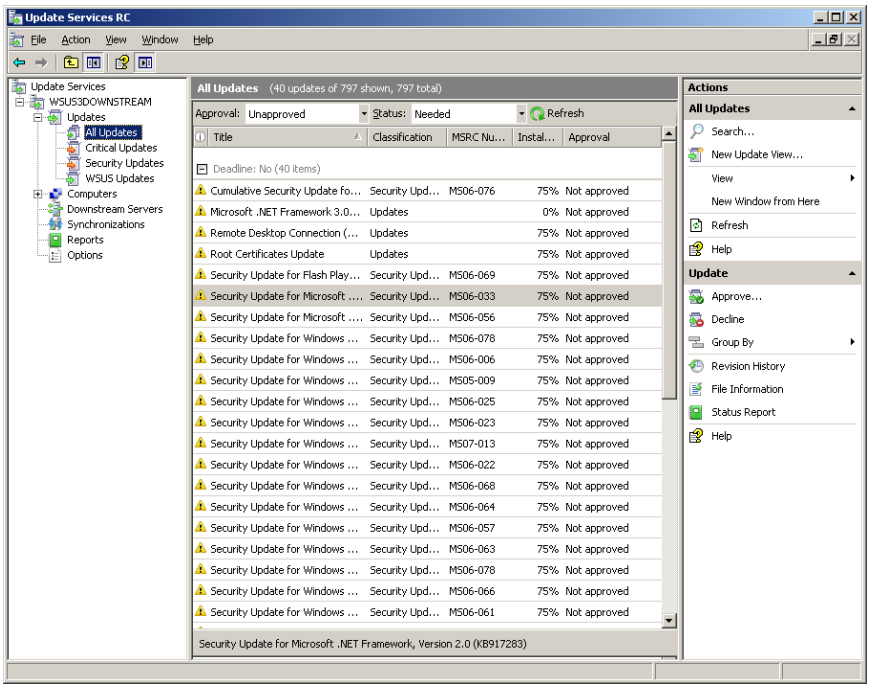


- **Approval** to list the updates by Approval status, such as Not Approved:

Copyright © 2008 Microsoft Corporation.
All rights reserved.



- **Deadline** to list the updates by a pre-configured Deadline, as applicable:



Approving the Updates

After updates have been synchronized to the WSUS server, they will be scanned automatically for relevance to the server's client computers. However, administrators must approve the updates manually before they are deployed to the computers on the network. When administrators approve an update (essentially telling WSUS what to do with it) choices are **Install** or **Decline** for a new update. Administrators can approve updates for the **All Computers** group or for subgroups. If an update is not

Copyright © 2008 Microsoft Corporation.

All rights reserved.

specifically approved, its approval status remains **Not approved**, and the WSUS server will simply allow clients to evaluate whether or not they need the update.

Note: If the WSUS server is running in replica mode, administrators will not be able to approve updates on the WSUS server.

Administrators can approve the installation of updates for all the computers in the WSUS network or for different computer groups. After approving an update, administrators can do one (or more) of the following:

- Apply this approval to child groups, if any.
- Set a deadline for automatic installation. When selecting this option, specific times and dates to install updates is set, overriding any settings on the client computers. In addition, administrators can specify a past date for the deadline to approve an update immediately (to be installed the next time client computers contact the WSUS server).
- Remove an installed update if that update supports removal.

Warnings:

- Administrators cannot set a deadline for automatic installation for an update if user input is required (for example, specifying a setting relevant to the update). To determine whether an update will require user input, look at the **May request user input** field in the update properties summary at the bottom for each individual update displayed on the **Updates** page. Also check for a message in the **Approve Updates** box which says "**The selected update requires user input and does not support an installation deadline**."

- If there are updates to the WSUS server component, administrators cannot approve other updates to client systems until the WSUS update is approved. Administrators will see the warning message in the Approve Updates dialog box: "**There are WSUS updates that have not been approved. You should approve the WSUS update before approving this update**." In this case, administrators should select the WSUS Updates node and make sure that all the updates in that view have been approved before returning to the general updates.

To approve updates

1. In the Update Services interface on either the Upstream or Downstream server, expand Updates and click All Updates to obtain the list of all updates.

   Note: Updates must be approved on the Upstream server before attempting to approve on the Downstream server(s) in order for the process to work properly without error messages.

2. In the list of updates, select one or more updates to approve:
   - **Right-click** an individual update from the list to highlight, or
   - Select multiple by moving the cursor over each update to select and hit control click, or
   - Select all by highlighting the first one and then scroll down to the end of the list with the shift key depressed and click on the last update.

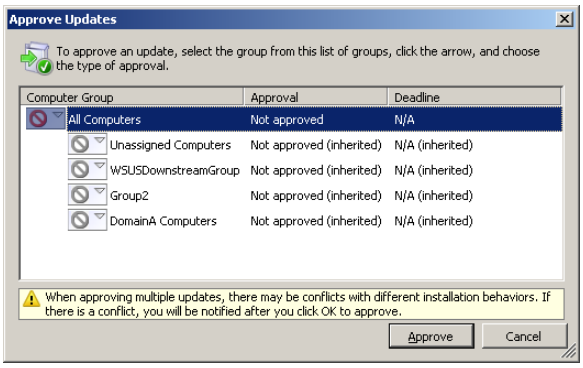
   Note: When approving multiple updates, there may be conflicts with different installation behaviors. If there is a conflict, the authorized administrator applying the updates will be notified after clicking OK to approve.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

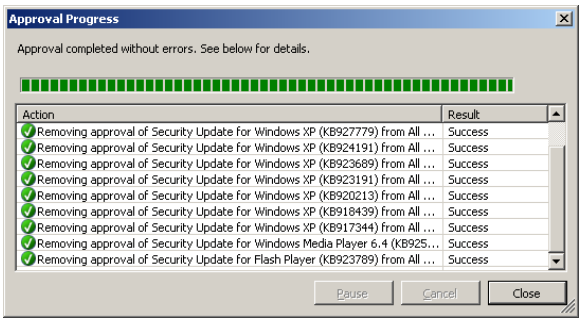
3. For the highlighted updates selected go to the Actions pane and click on Approve… under Update to bring up the Approve Updates page.
4. Click on All Computers to approve the update(s) for All Computers and click Approve.

Note: Clicking on anything other than All Computers negates the default approval/deadline inheritance policy, such that it would be rare for an authorized administrator to select anything other than All Computers.

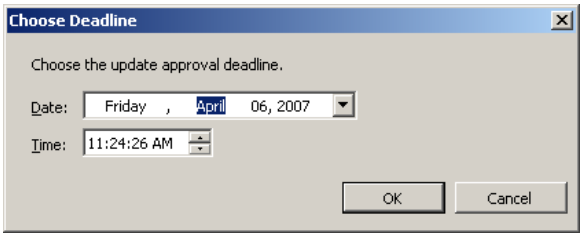


Note: Clicking on the down arrow in front of All Computers will bring a drop-down menu with the following options: Approved for Install; Approved for Removal; Not Approved; Deadline, with arrow to separate drop-down window that reflects None, One week, Two weeks, One Month, Custom…; Same as Parent; and Apply to Children.

5. This action brings up the Approval Process window that reflects Action and Result.



6. Any errors in processing the selected updates for approval will be displayed and can be viewed by scrolling down the list.
7. Click Close to save/exit.
8. To identify the update(s) to be installed as soon as the client computers contact the server, click on the down arrow in front of All Computers to bring up the drop-down list.
9. Click Deadline from the drop-down list and scroll over and click Custom… from the new drop-down list to bring up the Choose Deadline page.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

10. Enter desired date and time and click OK to save and click Approve in the Approve Updates page to process.
11. This option will bring up the Approval Progress page reflected above.
12. Click Close to save/exit.

Unapproving Updates

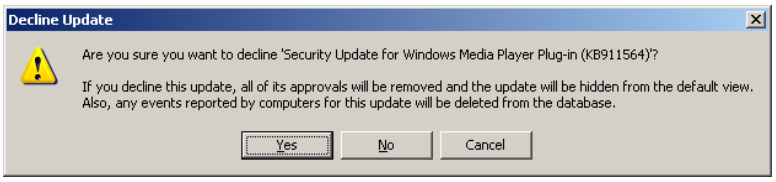
If an update has been approved and it is decided not to install it at this time, but want to save it for a future time, administrators can unapprove the update. This means that the update will remain in the default list of available updates and will report client compliance, but will not be installed on clients.

To unapprove updates - option A

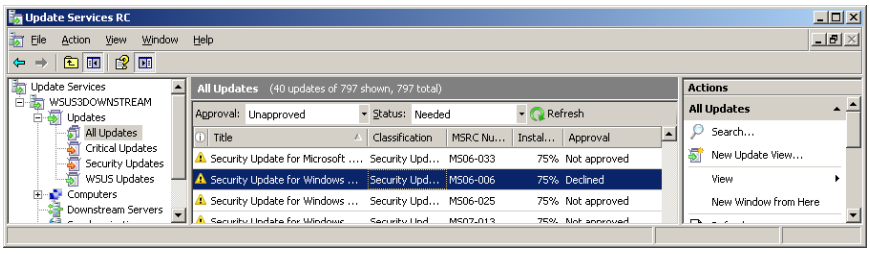
1. In the Update Services interface, expand Updates and double-click on All Updates to bring up the update listing.
2. In the list of updates, select one or more updates (as described in the approval process) to unapproved.

Note: Updates must have been previously **Approved** in order to proceed.

3. Right-click on highlighted update(s) to bring up the drop-down list and click on Decline to bring up the Decline Update page.



4. In the Decline Update page, click Yes to save/exit.
5. Verify the approval status has changed to **Declined** in the update list.



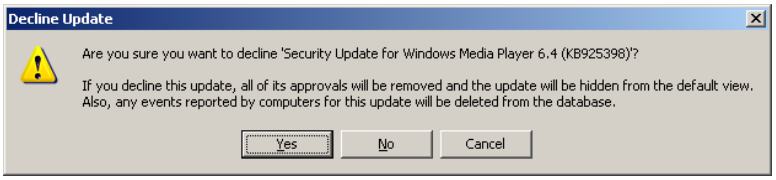
To unapprove updates - option B

1. In the Update Services interface, expand Updates and double-click on All Updates to bring up the update listing.
2. In the list of updates, select one or more updates (as described in the approval process) to unapprove.

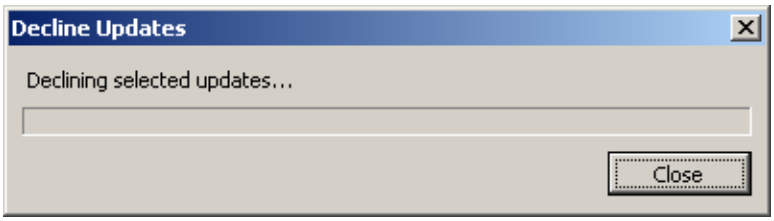
Note: Updates must have been previously **Approved** in order to proceed.

3. In the Actions pane, right-click on Decline to bring up the Decline Update page.

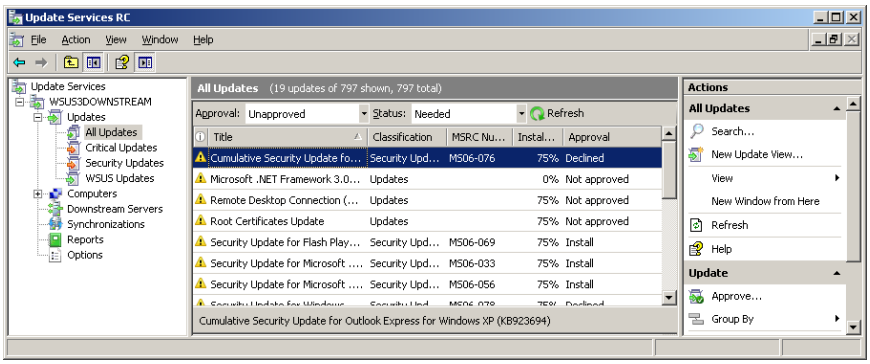
Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. Click Yes on the Decline Update window confirmation message to start the process.



5. Review the updates listing to verify that the update previously reflected as Install now reflects Declined.

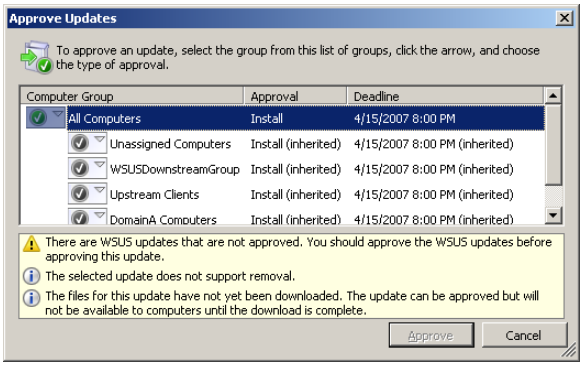


Selecting a deadline for updates

Deadlines can only be applied to Updates approved for Install on the Upstream Server, and only Approved for Install (e.g., those with the **Install** approval status) may be selected to apply a deadline to.

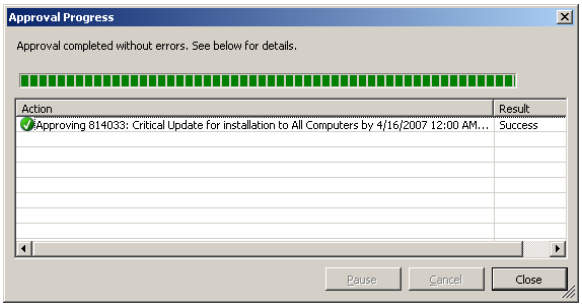
To select deadline

1. In the WSUS Upstream administrative console, expand Updates and double-click on All Updates to bring up the update listing.
2. In the list of updates, select one or more Install updates to set Deadline on by highlighting, right-clicking and selecting Approve to bring up the Approve Updates page for that particular update.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. In the Approve Updates page, select the computer(s) to apply the change and from the drop-down list, select Deadline. In the new drop-down list, select periodicity to apply to the deadline as either None, One Week, Two Weeks, One Month or Custom and click Approve to bring up the Approval Progress page.



4. Click Close to exit.

Note: Under Action, the approval will be reflected and the date (one week out in this case) added to the update to reflect the imposed Deadline established.

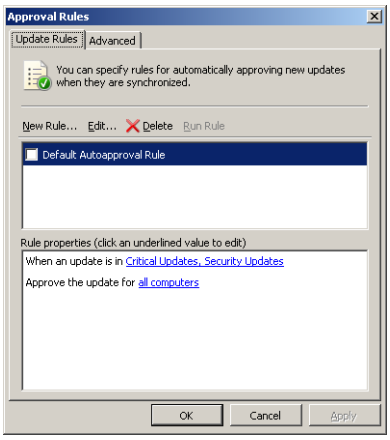
Approving Updates Automatically

Administrators can configure the WSUS server for automatic approval of certain updates. Administrators can also specify automatic approval of revisions to existing updates as they become available. This option is selected by default. A revision is a version of an update that has had changes made to it (for example, it might have expired, or its applicability rules might have changed). If administrators do not choose to approve the revised version of an update automatically, WSUS will use the older version, and administrators must manually approve the update revision.

Administrators can create a rule that the WSUS server will automatically apply during synchronization. Administrators specify what updates to automatically approve for installation, by update classification and by computer group. This applies only to new updates, as opposed to revised updates. This setting is available on the **Options** pane, under **Automatic Approvals**.

To automatically approve updates

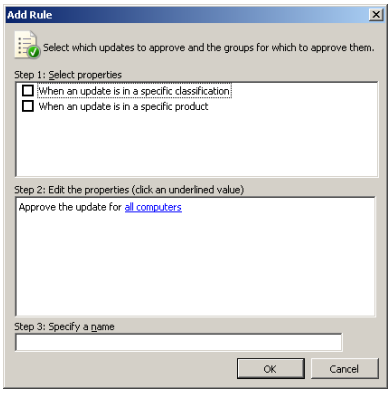
1. In the Update Services interface for the Upstream and/or Downstream Server(s), click **Options** and select **Automatic Approvals** from the Options pane (center) to bring up the Approval Rules page.



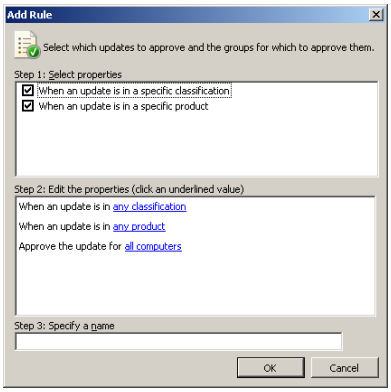
2. In the default Update Rules tab, click on **New Rule…** to bring up the Add Rule page.

Copyright © 2008 Microsoft Corporation.

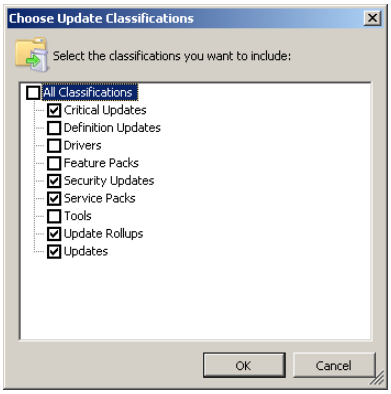
All rights reserved.



3. Under **Step 1: Select properties** of the Add Rule page, select whether to use update classifications or products (or both) as criteria.

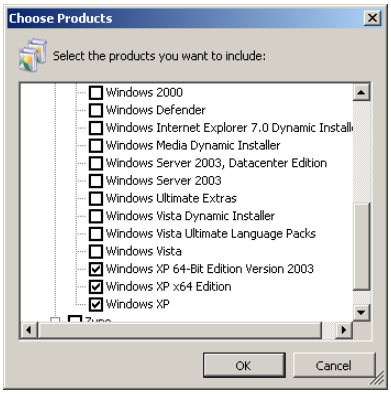


4. Under **Step 2: Edit the properties**, click on the underlined properties to select the values for which automatic approvals are desired, such as:

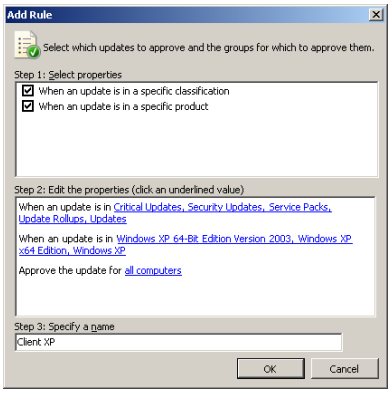


And/or,

Copyright © 2008 Microsoft Corporation.
All rights reserved.

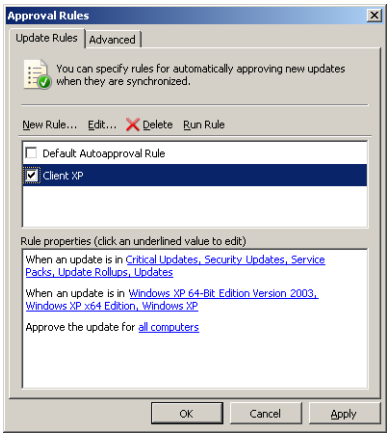


5. Click **OK** to save/continue and under **Step 3: Specify a name**, enter a name to apply to this Automatic Approval rule and click **OK**.



6. Verify that the options selected now reflect in **Step 2: Edit the properties** and that the name is reflected in **Step 3: Specify a name** and click **OK**.

7. Highlight the Approval Rule created and click **OK** to save/exit.



Automatically Approving Revisions to Updates and Declining Expired Updates

The **Automatic Approvals** section of the **Options** pane contains a default option to automatically approve revisions to approved updates. Administrators can also set the WSUS server to automatically decline expired updates. If administrators choose not to approve the revised version of an update automatically, the WSUS server will use the older revision, and an administrator must manually approve the update revision.

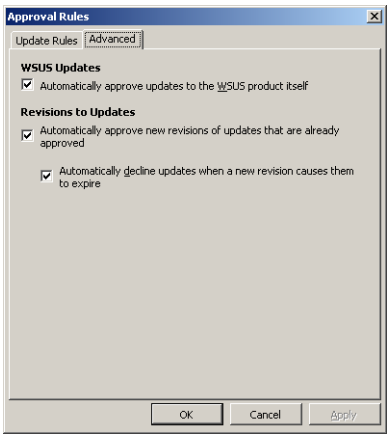
Copyright © 2008 Microsoft Corporation.

All rights reserved.

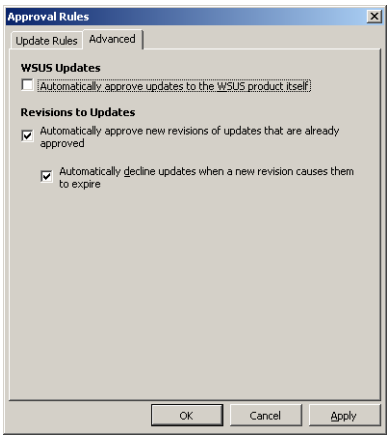
Note: A revision is a version of an update that has changed (for example, it might have expired or have updated applicability rules).

To automatically approve revisions to updates

1. In the Update Services interface for the Upstream and/or Downstream Server(s), click **Options** and select **Automatic Approvals** from the **Options** pane (center) to bring up the Approval Rules page and then click on the **Advanced** tab



2. On the Advanced tab, ensure both **Automatically approve new revisions of approved updates** and **Automatically decline updates when a new update causes them to expire** are selected and click **OK** to save/exit.



Warning: It is recommended that the default value for these options be kept, that is, that revisions are automatically approved and expirations are automatically declined.

Declining Updates

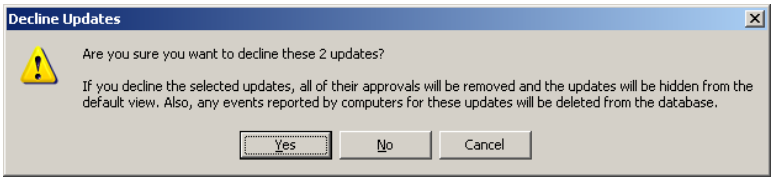
If this option is selected, the update is removed from the default list of available updates and the WSUS server will not offer the update to clients, either for evaluation or install. Administrators can reach this option by selecting an update or group of updates and right-clicking or going to the Actions pane. Declined updates will appear in the updates list only if an administrator selected **Declined** in the Approval list when specifying the filter for the update list under View.

Copyright © 2008 Microsoft Corporation.

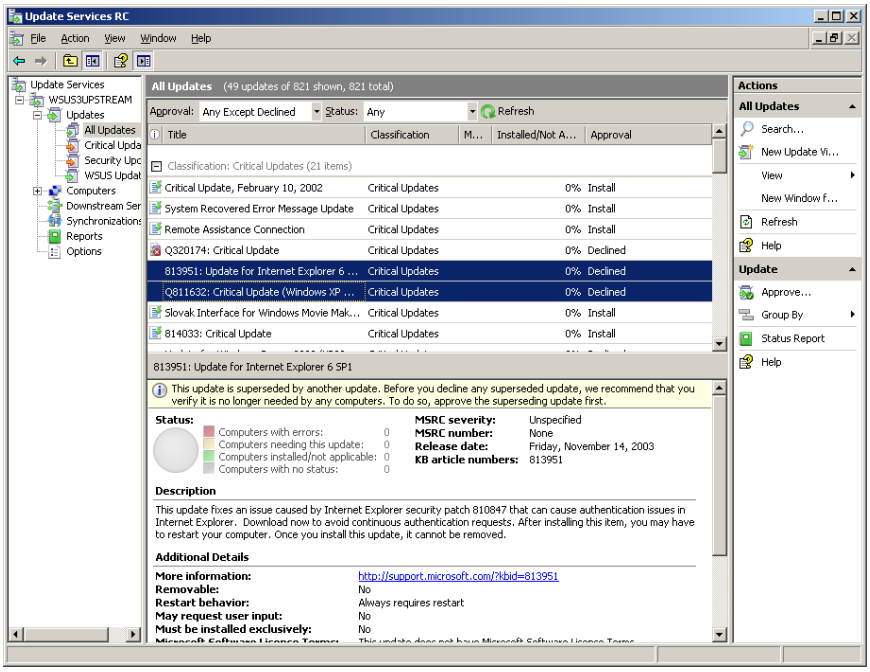
All rights reserved.

To decline updates

1. In the Update Services interface of either the Upstream or Downstream Server(s), click **Updates** to expand the node and **All Updates** to reflect the listing.
2. In the list of updates, select one or more updates identified as **Install** to decline. In the Actions pane, click on **Decline** and in the **Decline Updates** page, click **Yes** to acknowledge/continue.



3. Verify that the Approval status has now changed to **Declined**.



Running WSUS 3.0 in Replica Mode

A WSUS server running in replica mode inherits the update approvals and computer groups created on its parent WSUS administration server. Administrators will typically have a single parent server with one or more downstream replica WSUS servers. Administrators approve updates and create computer groups on the parent server, which the replica servers will then mirror.

Administrators may now designate any WSUS server as a downstream replica at any time. In the Update Services interface, select **Options**, then **Update Source and Proxy Server**, and on the **Update Source** tab select **Synchronize from another Windows Server Update Services server**, then **This server is a replica of the upstream server**.

Administrators will be able to perform only limited administration capabilities on a WSUS replica server, which will primarily consist of:

- Adding and removing computers from computer groups. A replica server inherits the computer groups that were created on the administration server. Administrators must assign the replica server's client computers to the computer groups.

Copyright © 2008 Microsoft Corporation.

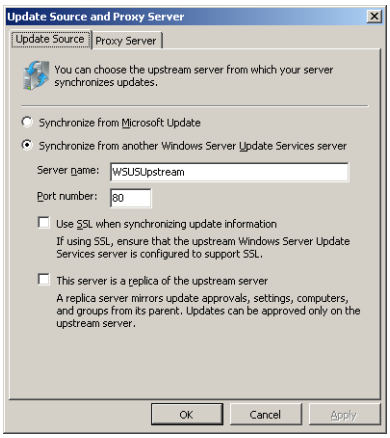
All rights reserved.

- Setting a synchronization schedule.
- Specifying proxy-server settings.
- Specifying the update source. This can be a server other than the administration server.
- Viewing available updates.
- Monitoring update, synchronization, and computer status, and monitoring WSUS settings on the server.

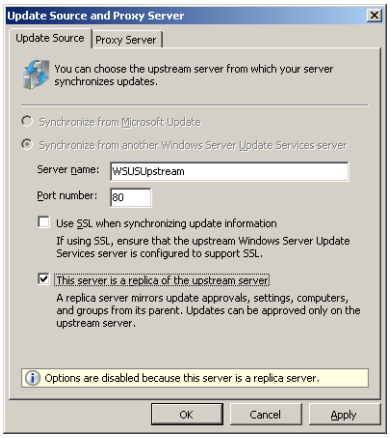
All standard WSUS reports are available on replica mode servers.

Create Replica Server

1. In the Update Services interface of a Downstream Server(s), select **Options**, then click **Update Source and Proxy Server** to bring up the Update Source and Proxy Server page.



2. In the **Update Source** tab, select **Synchronize from another Windows Server Update Services server**, then **This server is a replica of the upstream server**.



3. Click **OK** to save/exit.

Note: Options are disabled because this server is a replica server is displayed.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Schedule Update Installations

In managing the process of updating computers (which includes WSUS servers), one of the main goals is to have any planned downtime occur when there is little chance for lost productivity. The following are suggestions for accomplishing this:

- To update WSUS servers or specific computers efficiently, put the WSUS servers or computers in their own computer group, and deploy to that group with a deadline set for a time when it is feasible for the WSUS servers or computers to be down (for example, on Sunday at 3:00 A.M).
- Deploy updates by using a deadline in the future. For example, set the WSUS servers or computers with a scheduled installation at a time when it is feasible for them to be briefly offline (for example, on Sunday at 3:00 A.M).
- Configure client computers or WSUS servers through Group Policy to immediately install updates that do not require a restart. (Before approving an update for installation, administrators can read the **Description** field in the properties for an update in order to determine whether the update will require restarting the computer. Administrators can view the properties for an update by selecting it in the list of updates on the **Updates** page in the WSUS console.) Enable the policy to install immediately any updates that do not require a computer restart, so that they are installed every day. Computers can then install any updates that do not interrupt service when they are ready to install (that is, scheduling for Sunday morning installation would be unnecessary). The tile of this policy is **Allow Automatic Updates immediate installation** (see the table earlier in this topic for more information).

Note: For maximum control over when servers are restarted as necessitated by an update installation, set Group Policy to Download the updates automatically and notify when they are ready to be installed, and then create a script that enables to an administrator accept and install the updates and then restart the computer on demand.

Some updates require a computer restart after they are installed (and, by default, will restart computers 5 minutes after they are installed.)

Warning: By not restarting servers after installing these updates, they are left at risk. However, depending on network configuration, it might also be risky to restart servers automatically, since many other resources in the network could depend on a single server. In this case, it might not be feasible to schedule automatic scheduled restarts of the server.

There are a couple of Group Policies that enable administrators to configure when a computer is restarted. However, when talking about servers, these policies have some limitations over control:

- No auto-restart for scheduled Automatic Updates installations—this policy will prevent automatic restarts of the server, and will enable manual restart—however, administrators have to log on to the server and then initiate the restart. This might not be practical if the server is typically unattended.
- Delay restart for scheduled installations—this policy can delay the time between the update installation and the computer restart, however, the maximum time that can be set here is 30 minutes.

If these are issues, consider the following procedure:

1. Use Group Policy to configure automatic download, and manual installation of the updates by enabling the Configure Automatic Updates Group Policy setting by selecting the Download the updates automatically and notify when they are ready to be installed option.
2. Create a script to automate installing the updates and then restarting of the server. This script would have the effect of a "button" to push to initiate all this, therefore the updates install and the server restarts when the script is executed. Administrators can do this at the most appropriate time.

In an Active Directory environment, administrators can use Group Policy to configure Automatic Updates and WSUS environment options by using the Windows Update settings. If Group Policy is used to configure Automatic Updates, the Automatic Updates user interface is disabled on the client computer.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Use Group Policies to configure Automatic Update settings on WSUS 3.0 clients

There are two methods to configure Automatic Updates on computers in order to allow the management of updates for those computers through a WSUS 3.0 server:

- Configure Automatic Updates via Group Policy. This method involves configuring domain-level Group Policies for computers within a domain, or local Group Policies on computers that are not in a domain.
- Configure Automatic Updates locally by modifying registry settings on the local computer. This method involves using the Registry Editor and is not used in the TOE. Configuring Automatic Updates via a local Group Policy has the same effect as using the Registry Editor.

Procedures for configuring Automatic Updates settings for WSUS 3.0 via a Group Policy object (GPO) are provided in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

Reports in Windows Server Update Services 3.0

Reports are an important part of managing WSUS 3.0. Administrators can keep track of nearly every aspect of the WSUS network by means of reports. The most important kinds of reports are:

- **Summary compliance reports** (the number of computers that need to install updates and the number of updates missing from computers). Administrators can generate these reports from the root node of the Update Services interface.
- **Individual computer reports**. Administrators can generate these reports by right-clicking the computer in the **Details** pane.
- **Individual update reports**. Administrators can generate these reports by right-clicking the update in the **Details** pane.
- **Downstream server summary compliance reports**. Administrators can generate these reports right-clicking the server in the **Details** pane.
- **Synchronization reports**. Administrators can generate these reports by right-clicking the synchronization in the **Details** pane.

Terminology for Update Status

Administrators can access update status from various locations in the WSUS console. The following table defines each possible status that can be reported by WSUS for an update. Typically, WSUS presents update status for a particular computer (for example, the status of an update on one computer) or computer group (for example, status for the five computers in Computer Group X on which the update has been installed). Administrators can filter the default views of computers or updates by update status, and in some cases by combinations of statuses (Failed or Needed, Installed/Not Applicable or No Status, and so on). Update status definitions are provided in the table below.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Update Status	Definition
Installed	The update is installed on the computer.
Needed	When referring to the status of one computer, Needed means the update is compatible with (and should be installed on) the computer. When referring to status for a computer group, the **Needed** column displays the number of computers in the group to which the update is applicable. Additionally, a positive Needed result means, technically, that as of the last time client computers made contact with the WSUS server, the update was determined to be applicable, but has not been installed. Therefore, it is possible that any of the following could be true when the status for an update is Needed: The update is approved for installation but the client computers have not yet contacted the WSUS server since the change was made. The update is not yet approved for installation, although the Detect only action has been performed. The update has already been downloaded and installed, but the client computer has not contacted the WSUS server since the update was installed. The update has already been downloaded and installed but the update requires that the client computer be restarted before changes go into effect, and the client computer has not yet been restarted. The update has been downloaded to the computer but not installed. The update has been neither downloaded nor installed on the computer.
Installed/Not Applicable	When referring to the status of one computer, Installed/Not Applicable means the update is not applicable to or required by that computer. When referring to the status for a computer group, the Installed/Not Applicable column displays the number of computers in the group for which the update is not applicable or not required.
No status	Typically, this means that since the time that the update was synchronized to the WSUS server, the computer has not contacted the WSUS server.
Failed	An error occurred when either a detection or an installation was attempted on the computer for the update.
Last contacted	This is the date on which the computer last contacted the WSUS server.

Creating Reports

Reports enable authorized administrators to monitor different aspects of the WSUS network: updates, client computers, and downstream servers. If a WSUS server has replica servers, administrators can choose to roll up the replica servers' client status to the upstream server.

Administrators can generate reports from the Reports page, as described below, and can also generate an update status report by double-clicking a specific update in an update list or right-clicking the update and choosing **Status Report**. Administrators can generate different kinds of update reports from different places in the administrative console (the Details section of a computer report, the details of a synchronization report, or the status preview pane for a computer). Administrators can generate a computer status report by double-clicking a specific computer in a computer list or right-clicking the computer and choosing **Status Report**. Administrators can generate different kinds of computer reports from different places in the administrative console.

Administrators can generate three kinds of report, as described in the following table.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Report Name	Function
Update Reports	View update status.
Computer Reports	View computer status.
Synchronization Reports	View the results of the last synchronization.

Update Reports

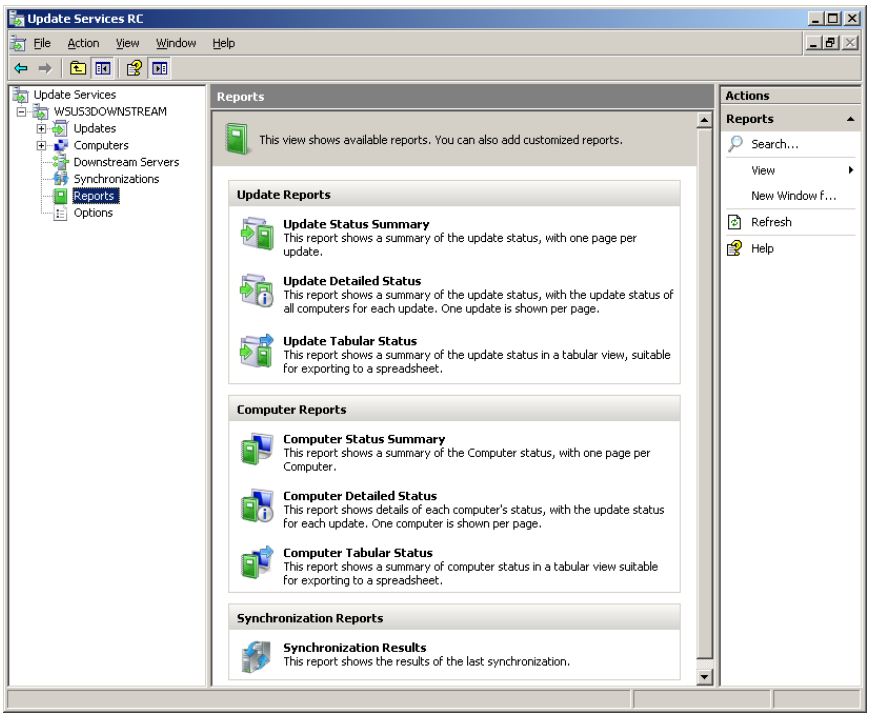
Update reports show the status for updates. Administrators can view the report in three ways: summary, detailed, and tabular; and can also filter the report by update classification, product, target computer group, or update installation status.

The report displays information from the most recent contact between client computers and the WSUS 3.0 server. The frequency with which client computers contact the WSUS 3.0 server is configured through Group Policy. By default, this is every 22 hours. Unless the contact frequency for client computers needs to be changed, generate this report the day after updates are approved to reflect latest approvals.

To run an update report

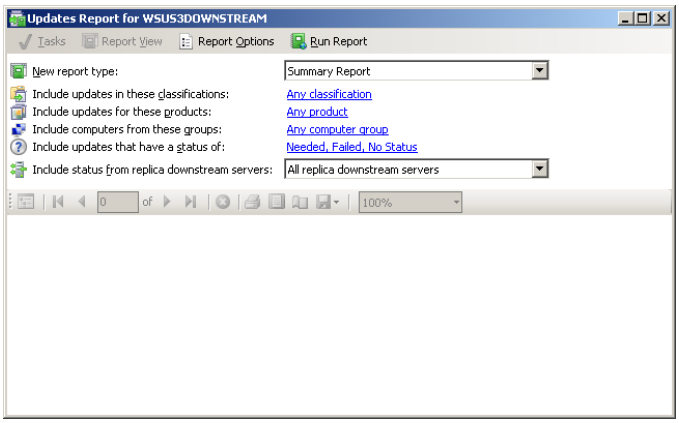
Reports can be generated on either Upstream or Downstream servers, depending on desire/need.

1. In the Update Services interface, select the **Reports** node to display the available Reports in the center pane



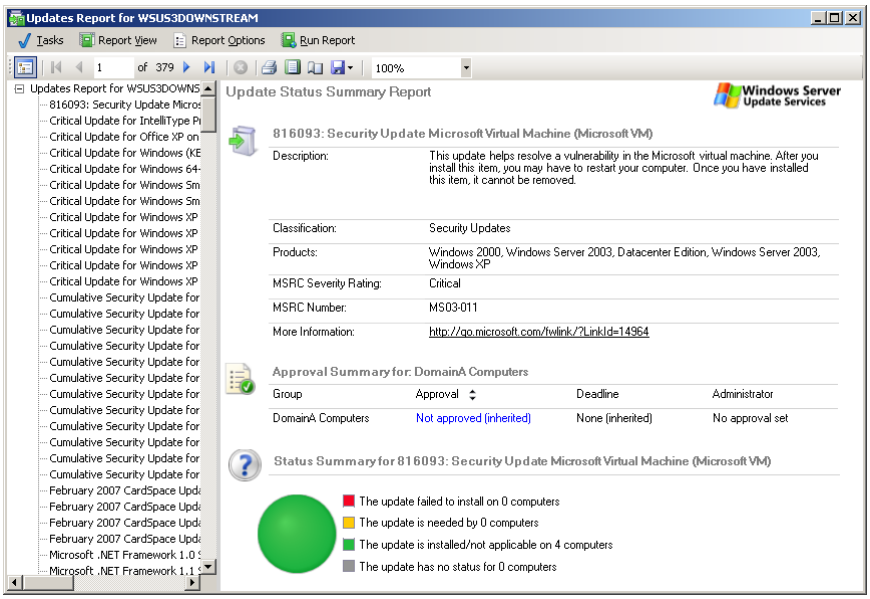
2. In the **Reports** pane, double-click **Update Status Summary** to display an overview update report.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



3. In the Updates Report window, configure the updates desired by classification, product, computer group, or update installation status.
4. Configure Summary Report by classifications; products; group; and/or status for desired outcome and click Run Report.

Note: Wait for report to be generated.



Note: By default, the left pane of the report is not expanded; however, sample expanded the **Updates Report for…** in order to display all information provided in the report.

The Update Status Summary view contains the elements listed in the following table.

Copyright © 2008 Microsoft Corporation.

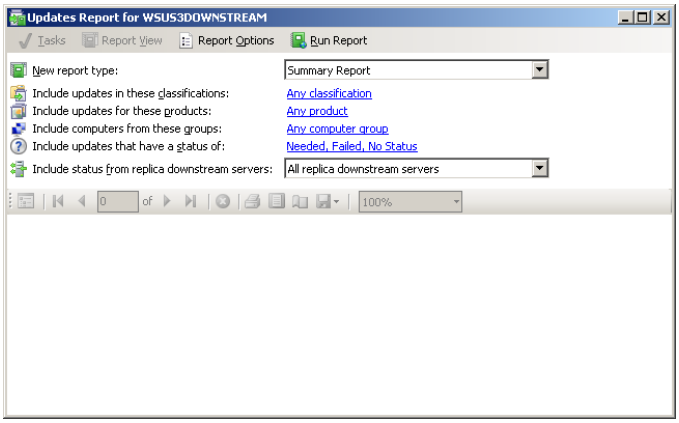
All rights reserved.

Column Name	Description
Updates Report tree view	The tree listing all the updates in the report.
Title	The title of the update.
Description	The description of the update.
Classification	The classification of the update.
Products	The product(s) to which the update applies.
MSRC Severity Rating	Microsoft Security Response Center rating.
MSRC Number	Microsoft Security Response Center identification number.
More information	Redirection to the relevant Web site.
Approval Summary for Computer Group	The listing of groups and approvals.
Group	The computer group.
Approval	Approval status (Approved, Not approved, Declined).
Deadline	The date by which the update must be installed.
Administrator	The administrative action.

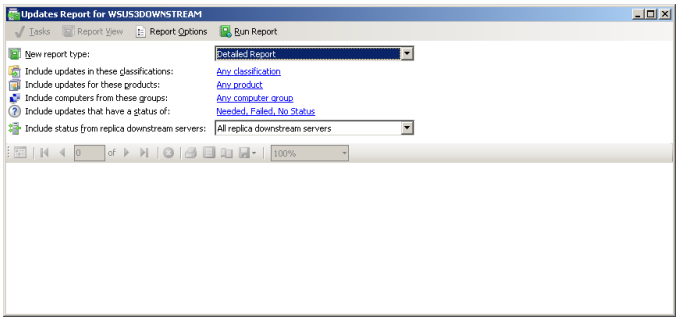
Change the View of Update Status Summary report

The view of an Update Status Summary report can be changed to a detail view or a tabular view by clicking **Report View** in the **Updates Report** toolbar.

1. In the **Reports** pane, double-click **Update Status Summary** to display an overview update report.



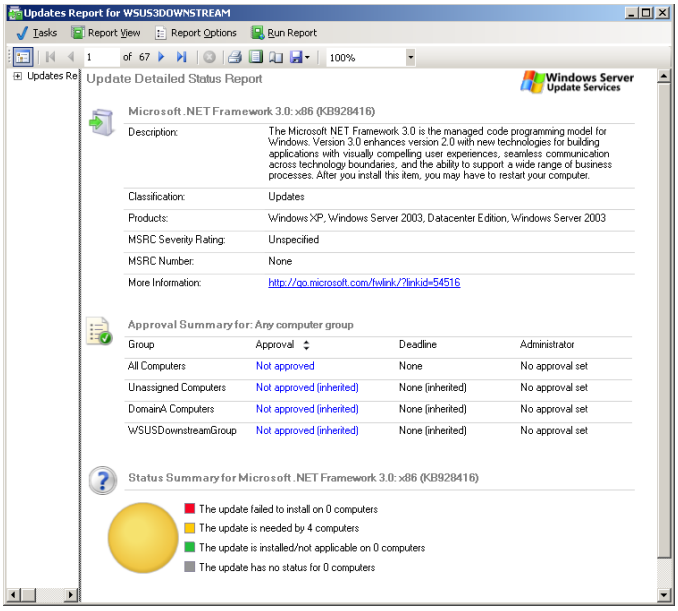
2. Click on the drop-down window next to New report type: to select Detailed Report.



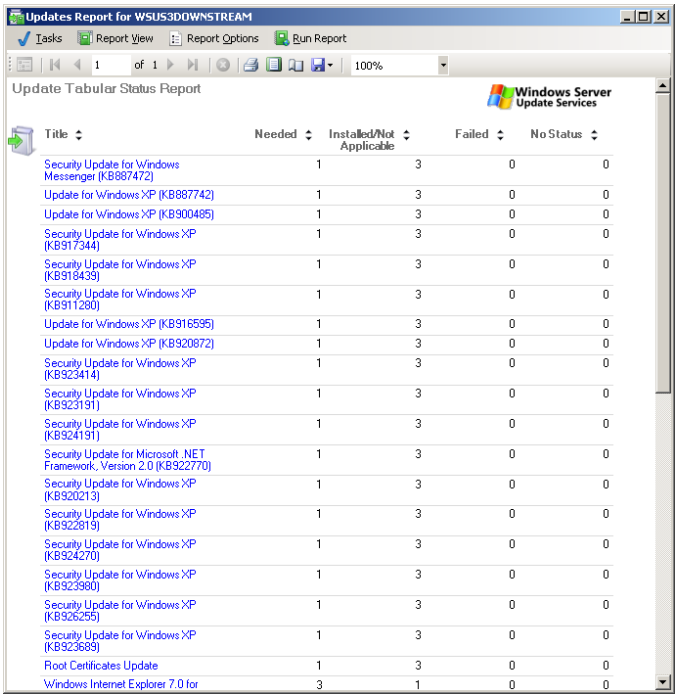
Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. Click on Run Report to process/view



4. Or click on the Tabular Report option and click Run Report to process/view.



Printing the report

Administrators can print the report in update summary, detailed, or tabular views, depending on how the update status report was configured.

1. On the **Updates Report** toolbar, click the printer icon.
2. In the **Print** dialog, select the necessary options and click **Print**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Computer Status Reports

The Computer Status report provides an update status summary for specified computer(s).

1. In the Update Services interface, select the Reports node
2. In the **Reports** pane, click Computer Status Summary to display an overview computer report.

Note: This report is identical to the **Update Status Summary** report identified previously, where all the same parameters apply. Therefore, they are not repeated herein (i.e., options; report type; classifications; etc.). The only difference is that the report is titled **Computers Report for…**

Synchronization Results Report

The Synchronization Results report enables administrators to see synchronization information for server(s) for a given time period, including errors that occurred during synchronization and a list of new updates. In addition, administrators can get general, status, and revision information for each new update.

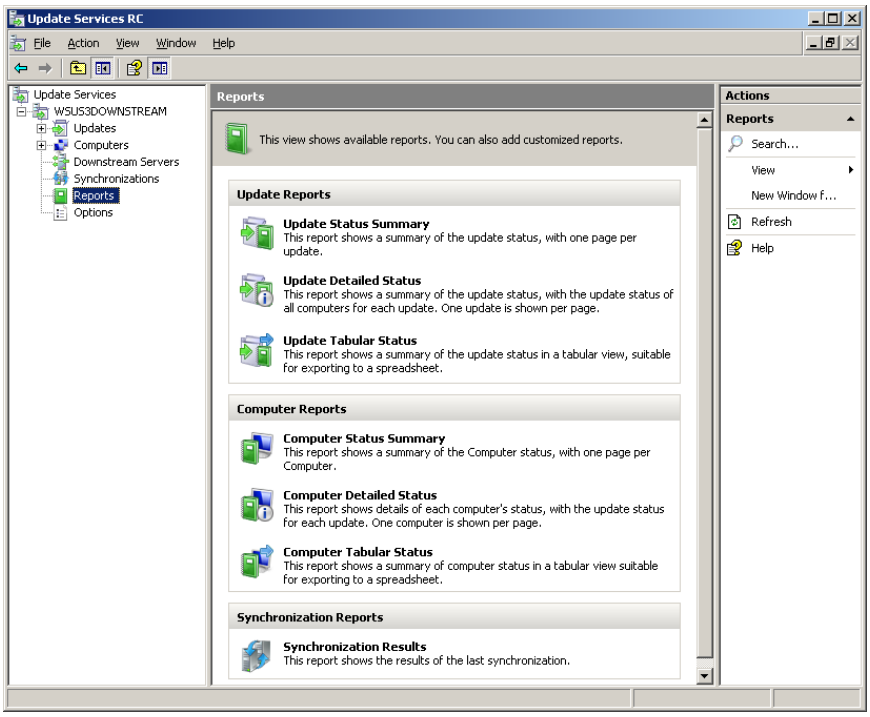
The report has four components, which are described in the following table.

Component Name	Purpose
Report Options	Shows the start and end dates of the period shown in the report, as well as the date of the report and the server for which the report was made.
Synchronization Summary	Displays summary information the numbers of new, revised, and expired updates in each synchronization
New Updates	Displays the new updates that have been synchronized to the WSUS server during the report's time period. Administrators can view the properties for each update by clicking the update. An update status report will be generated for that individual report.
Revised Updates	Displays the revised updates that have been synchronized to the WSUS server during the report's time period. Administrators can view the properties for each update by clicking the update. An update status report will be generated for that individual report.
Expired Updates	Displays the updates that have been expired during the report's time period.

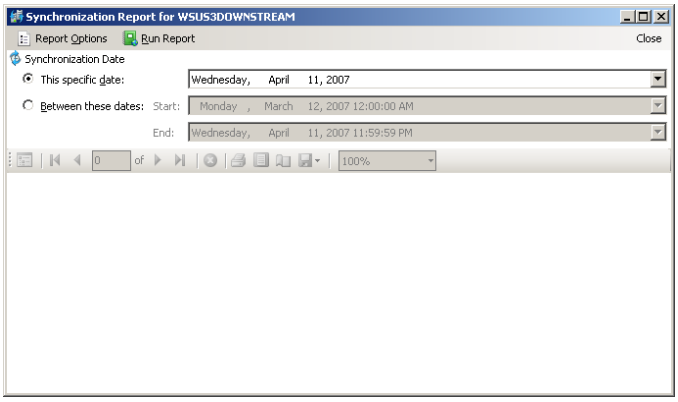
1. In the Update Services interface, select the Reports node to display the available Reports in the center pane.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



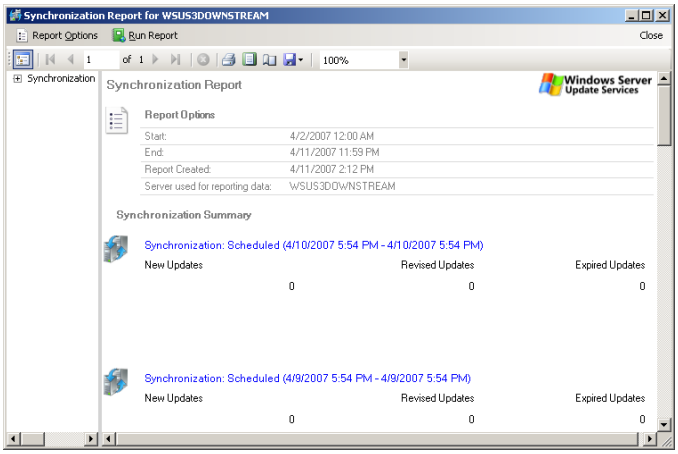
2. In the **Reports** pane, double-click **Synchronization Results** to display an overview update report. By default, the report displays any synchronizations done the day of report generation.



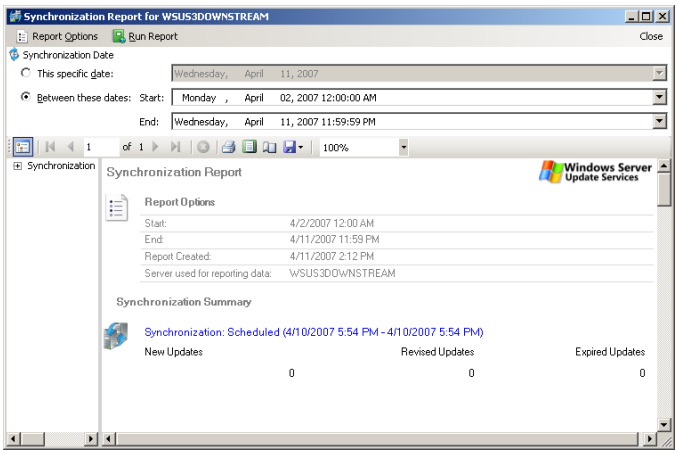
3. To change synchronization period for the report, click the radio button before **Between these dates:** and specify the dates to be included. Click **Run Report**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



4. Clicking on **Report Options** only changes the view of the report, such as:



Forests and Domains

The Active Directory service is a distributed database that stores and manages information about network resources, as well as application-specific data from directory-enabled applications. Active Directory allows administrators to organize objects of a network (such as users, computers, and devices) into a hierarchical collection of containers known as the logical structure. The top-level logical container in this hierarchy is the forest. Within a forest are domain containers, and within domains are organizational units.

Understanding domains and forests requires understanding the possible relationships they might have in Active Directory. The relationships between these logical containers might be based on administrative requirements, such as delegation of authority, or they might be defined by operational requirements, such as the need to provide for data isolation. Active Directory service administrators can use domain and forest containers to meet a number of specific requirements, including:

- Implementing an authentication and authorization strategy for sharing resources across a network;
- Providing a mechanism for centralizing management of multiple domains and forests;
- Providing an information repository and services to make information available to users and applications; and
- Organizing objects of a network (such as users, computers, devices, resources, and application specific data from directory-enabled applications) into a non-physical hierarchical structure.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The Logical Structure of Active Directory

Active Directory stores network object information and implements the services that make this information available and usable to users. Active Directory presents this information through a standardized, logical structure that helps establish the organization of domains and domain resources in a useful way. This presentation of object information is referred to as the logical structure because it is independent of the physical aspects of the Active Directory infrastructure, such as the domain controllers required for each domain in the network.

Components of the Logical Structure

The logical structure consists of leaf object and container object components that must conform to the hierarchical structure of an Active Directory forest. Leaf objects are objects that have no child objects, and are the most basic component of the logical structure. Container objects store other objects and occupy a specific level within the forest hierarchy.

The relationships among the components of the logical structure control access to stored data and determine how that data is managed across one or more domains within a single forest. The components that make up the Active Directory logical structure are described in the following table.

Components of the Active Directory Logical Structure

Component	Description
Organizational Units	OUs are container objects. These container objects are used to arrange other objects in a manner that supports administrative purposes. By arranging objects in OUs, it is easier to locate and manage them. The authority to manage an organizational unit can also be delegated. OUs can be nested in other organizational units. Objects that have similar administrative and security requirements can be arranged into OUs. OUs provide multiple levels of administrative authority, so that Group Policy settings can be applied and administrative control can be delegated. This delegation simplifies the task of managing these objects and enables the structuring of Active Directory to fit an organization's requirements.
Domains	Domains are container objects. Domains are a collection of administratively defined objects that share a common directory database, security policies, and trust relationships with other domains. In this way, each domain is an administrative boundary for objects. A single domain can span multiple physical locations or sites and can contain millions of objects.
Domain Trees	Domain trees are collections of domains that are grouped together in hierarchical structures. When a domain is added to a tree, it becomes a child of the tree root domain. The domain to which a child domain is attached is called the parent domain. A child domain might in turn have its own child domain. The name of a child domain is combined with the name of its parent domain to form its own unique DNS name such as Corp.nwtraders.msft. In this manner, a tree has a contiguous namespace.
Forests	A forest is a complete instance of Active Directory. Each forest acts as a top-level container in that it houses all domain containers for that particular Active Directory instance. A forest can contain one or more domain container objects, all of which share a common logical structure, global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. The first domain in the forest is called the forest root domain. The name of that domain refers to the forest, such as Nwtraders.msft. By default, information in Active Directory is shared only within the forest. In this way, the forest is a security boundary for the information that is contained in that instance of Active Directory.
Site Objects	Sites are leaf and container objects. The sites container is the topmost object in the hierarchy of objects that are used to manage and implement Active Directory replication. The sites container stores the hierarchy of objects that are used by the

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Components of the Active Directory Logical Structure	
Component	**Description**
	Knowledge Consistency Checker (KCC) to affect the replication topology. Some of the objects located in the sites container include NTDS Site Settings objects, subnet objects, connection objects, server objects, and site objects (one site object for each site in the forest). The hierarchy is displayed as the contents of the Sites container, which is a child of the Configuration container.

By understanding the purpose and hierarchical structure of these components, a variety of tasks can be completed, including installing, configuring, managing, and troubleshooting Active Directory. Although the logical structure of Active Directory is a hierarchical organization of all users, computers, and other physical resources, the forest and domain form the basis of the logical structure.

Forests, which are the security boundaries of the logical structure, can be structured to provide data and service autonomy and isolation in an organization in ways that can both reflect site and group identities and remove dependencies on the physical topology. Domains can be structured within a forest to provide data and service autonomy (but not isolation) and to optimize replication with a given region.

This separation of logical and physical structures improves manageability and reduces administrative costs because the logical structure is not impacted by changes in the physical structure, such as the addition, removal, or reorganization of users and groups.

Domains

Domains are logical directory components that can be created to manage the administrative requirements of an organization. The logical structure is based on the administrative requirements of an organization, such as the delegation of administrative authority, and operational requirements, such as the need to control replication. In general, domains are used to control where in the forest replication of domain data occurs and organizational units are used to further organize network objects into a logical hierarchy and delegate control to appropriate administrative support personnel.

A domain is a partition in an Active Directory forest. Partitioning data enables organizations to replicate data only to where it is needed. In this way, the directory can scale globally over a network that has limited available bandwidth. Domains can also be defined as:

- Containers within a forest
- Units of Policy
- Units of Replication
- Authentication and Authorization Boundaries
- Units of Trust

Each domain has a domain administrators group. Domain administrators have full control over every object in the domain. These administrative rights are valid within the domain only and do not propagate to other domains.

Domains as Containers within a Forest

Within the scope of a forest, a domain is a container. Objects in that container inherently trust each other and the security services located in that same container. Each time a new domain container is created in a forest, a two-way, transitive trust relationship is automatically created between the new domain and its parent domain. Trusts are logical relationships established between domains to allow pass-through authentication in which a trusting domain honors the logon authentications of a trusted domain. Because

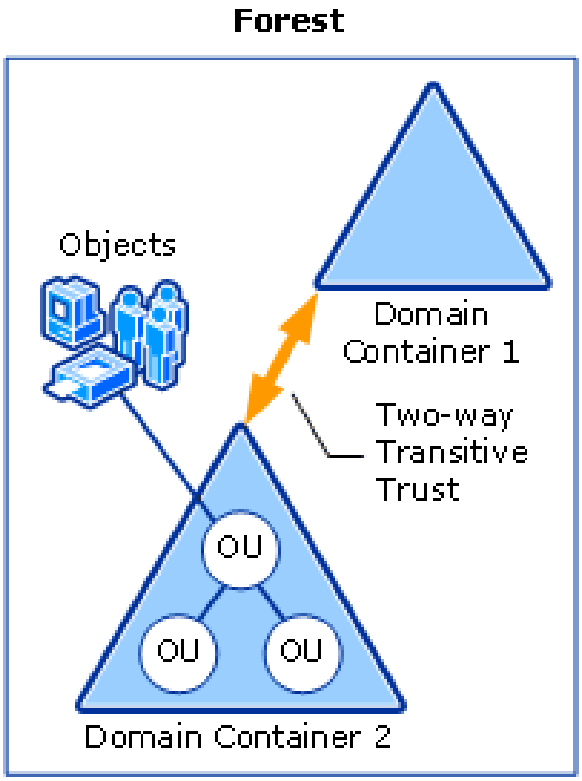
Copyright © 2008 Microsoft Corporation.

All rights reserved.

all domain containers within a forest are joined together by two-way transitive trusts, objects within one domain container also inherently trust all other objects and security services located in every domain container located in that forest.

Domain containers are used to store and manage Active Directory objects, some of which have a physical representation. All of the objects within the domain container are stored in a central database that stores only objects created within that domain. Some objects represent people or groups of people, while others represent computers or network servers. Examples of Active Directory objects that have a physical representation are user, computer, and group objects.

While domains contain objects that represent physical things, they also contain objects that are used to help self-regulate domain operations such as Trusted Domain Objects (TDOs) and site link objects. Domain containers can also hold subordinate containers such as organizational units. The following figure shows where objects are stored within the logical structure of a domain.



Organizational Units and Objects

Organizational units are used to group objects, including accounts and resources in a domain, for administrative purposes, such as the application of Group Policy or delegation of authority. Control over an OU, including the objects within it, is determined by the ACLs on the OU and on the objects in the OU.

Organizational Units

The OU is a particularly useful type of directory object contained within domains. Each OU is an ADcontainer within a domain into which users, groups, computers, and other OUs of the domain can be placed. An OU cannot contain objects from other domains.

An OU is the smallest scope or unit to which Group Policy settings can be assigned or to which administrative authority can be delegated. A hierarchy of OUs can be extended as necessary to model

Copyright © 2008 Microsoft Corporation.

All rights reserved.

the hierarchy of an organization within a domain. The administrative model of the OU can be scaled to any size.

Administrative authority can be delegated for individual OUs or for multiple OUs. Organizational units can be nested to create a hierarchy within a domain and form logical administrative units for users, groups, and resource objects, such as printers, computers, applications, and file shares. The OU hierarchy within a domain is independent of the structure of other domains: Each domain can implement its own hierarchy. Likewise, domains that are managed by the central authority can implement similar OU hierarchies. The structure is flexible, which allows organizations to create an environment that mirrors the administrative model, whether it is centralized or decentralized.

Objects

Active Directory objects represent the physical entities that make up a network. An object stores an instance of a class. A class is defined in the Active Directory schema as a specific set of mandatory and optional attributes - that is, an attribute can be present in an object in Active Directory only when that attribute is permitted by the object's class. Classes also contain rules that determine which classes of objects can be superior to (parents of) a particular object of the class. Each attribute is also defined in the directory schema. The attribute definitions determine the syntax for the values the attribute can have.

Creation of an Active Directory object requires specification of values for the attributes of the object in its particular class, consistent with the rules of the directory schema. For example, creating a user object requires specification of alphanumeric values for the user's first and last names and the logon identifier, which are mandatory according to the directory schema. Other non-mandatory values can also be specified, such as telephone number and address.

Applications that create or modify objects in Active Directory use the directory schema to determine what attributes the object must and might have, and what those attributes can look like in terms of data structures and syntax constraints. The directory schema is maintained forest-wide so that all objects created in the directory conform to the same values.

Objects are either container objects or leaf objects. A container object stores other objects, and as such occupies a specific level in a subtree hierarchy. An object class is a container if at least one other class specifies it as a possible superior, so any object class defined in the schema can become a container. A leaf object does not store other objects, so it occupies the endpoint of a subtree.

Forests

At its highest level, a forest is a single instance of Active Directory. Therefore, a forest is synonymous with Active Directory, meaning that the set of all directory partitions in a particular Active Directory instance (which includes all domain, configuration, schema and optional application information) makes up a forest. This means that when there are multiple forests in an enterprise they will, by default, act separately from each other as if they were the only directory service in the organization.

This behavior, however, is easily be modified so that multiple forests can share Active Directory responsibilities across an enterprise. This is done by creating external or forest trust relationships between the forests. In this way, each forest can be connected with every other forest to form a collaborative directory service solution for any enterprise with business needs that include multiple forest collaboration.

Forests can also be defined as:

- Collections of Domain Containers that Trust Each Other
- Units of Replication

Copyright © 2008 Microsoft Corporation.

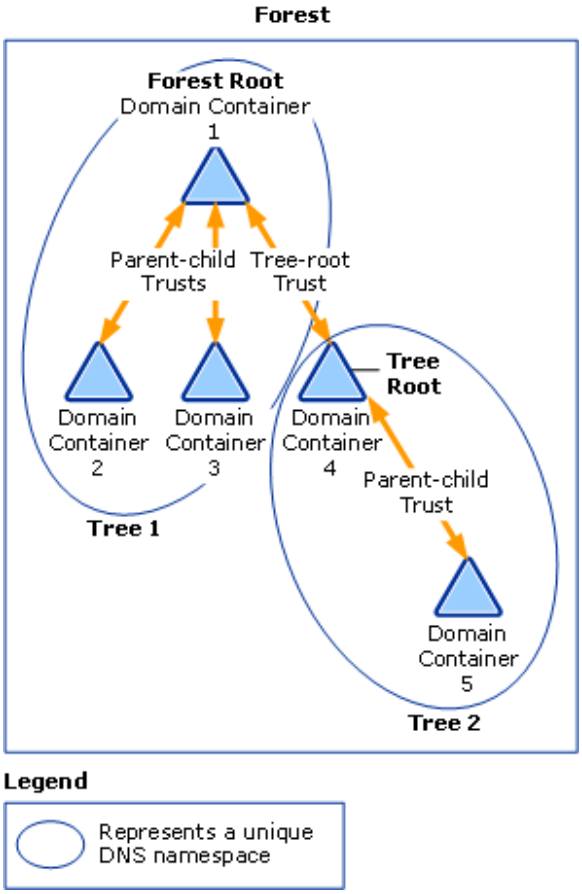
All rights reserved.

- Security Boundaries
- Units of Delegation

Forests as Collections of Domain Containers that Trust Each Other

Within the scope of Active Directory, a forest is a collection of domain containers that inherently trust each other and other security services that are located in that same forest. All domain containers in a forest share a common global catalog, directory schema, and directory configuration, as well as automatic two-way transitive trust relationships. Because all of the domain containers are inherently joined through two-way transitive trusts, all authentication requests made from any domain in the forest to any other domain in the same forest will be granted. In this way, all security principals that are located in domain containers within a forest inherently trust each other.

Forests can be used to segregate domain containers into one or more unique DNS namespace hierarchies known as domain trees. Although each domain tree consists of a unique namespace the schema and configuration data for the forest are shared throughout all the domain containers in a forest irrespective of namespace. Each domain container in a forest must adhere to DNS naming schemes and all domains are organized in a root and subordinate domain hierarchy. Root domains, such as forest root and tree root domains, define the DNS namespace for their subordinate domains. Although a forest can consist of multiple domain trees, it represents one organization. However, an organization can have multiple forests. As shown in the following figure, the namespace for each root domain must be unique.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

Forest Root domain

Although trees in a forest do not share the same DNS namespace, a forest does have a single root domain, called the forest root domain. The forest root domain is, by definition, the first domain created in the forest. The Enterprise Admins and Schema Admins groups are located in this domain. By default, members of these two groups have forest-wide administrative credentials. In Windows 2000 Active Directory, the forest root domain cannot be deleted, changed, or renamed. In Windows Server 2003 Active Directory, the forest root domain cannot be deleted, but it can be restructured or renamed.

Objects are located within Active Directory domains according to a hierarchical path, which includes the labels of the Active Directory domain name and each level of container objects. The full path to the object is defined by the distinguished name (also known as a DN). The distinguished name is unambiguous (identifies one object only) and unique (no other object in the directory has this name). By using the full path to an object, including the object name and all parent objects to the root of the domain, the distinguished name uniquely and unambiguously identifies an object within a domain hierarchy.

The distinguished name of the forest root domain is used to locate the configuration and schema directory partitions in the namespace. The distinguished names for the Configuration and Schema containers in Active Directory always show these containers as child objects in the forest root domain. For example, in the child domain Noam.wingtiptoys.com (where Wingtiptoys.com is the name of the forest root domain), the distinguished name of the Configuration container is cn=configuration,dc=wingtiptoys,dc=com. The distinguished name of the Schema container is cn=schema,cn=configuration,dc=wingtiptoys,dc=com. However, this naming convention provides only a logical location for these containers.

These containers do not exist as child objects of the forest root domain, nor is the schema directory partition actually a part of the configuration directory partition: They are separate directory partitions. Every domain controller in a forest stores a copy of the configuration and schema directory partitions, and every copy of these partitions has the same distinguished name on every domain controller.

Domain Trees

A domain tree represents a unique DNS namespace: it has a single root domain, known as the tree root domain, and is built as a strict hierarchy: Each domain above the tree root domain has exactly one superior, or parent, domain (the forest root domain). The namespace created by this hierarchy, therefore, is contiguous - each level of the hierarchy is directly related to the level above it and to the level below it. In other words, the names of domains created beneath the tree root domain (child domains) are always contiguous with the name of the tree root domain. The DNS names of the child domains of the root domain of a tree reflect this organization; therefore, the children of a root domain called Somedomain are always children of that domain in the DNS namespace (for example, Child1.somedomain, Child2.somedomain, and so forth).

Multiple domain trees can belong to a single forest and do not form a contiguous namespace; that is, they have noncontiguous DNS domain names. Although the roots of the separate trees have names that are not contiguous with each other, the trees share a single overall namespace because names of objects can still be resolved by the same Active Directory instance. A forest exists as a set of cross-reference objects and trust relationships that are known to the member trees. Transitive trusts at the root domain of each namespace provide mutual access to resources.

The domain hierarchy in a forest determines the transitive trust links that connect each domain. Each domain has a direct trust link with its parent and each of its children. If there are multiple trees in a forest, the forest root domain is at the top of the trust tree and, from a trust perspective, all other tree roots are children. That means authentication traffic between any two domains in different trees must pass through the forest root.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Child Domains

Child domains can represent geographical entities (for example, the United States and Europe), administrative entities within the organization (for example, sales and marketing departments), or other organization-specific boundaries, according to the needs of the organization. Domains are created below the root domain to minimize Active Directory replication and to provide a means for creating domain names that do not change. Changes in the overall domain architecture, such as domain collapses and domain re-creation, create difficult and potentially IT-intensive support requirements. A good namespace design should be capable of withstanding reorganizations without the need to restructure the existing domain hierarchy.

Each time a new child domain is created, a two-way transitive trust relationship (known as the parent-child trust) is automatically created between the parent and new child domain. In this way, transitive trust relationships flow upward through the domain tree as it is formed, creating transitive trusts between all domains in the domain tree. The parent-child relationship is a naming and trust relationship only. Administrators in a parent domain are not automatically administrators of a child domain. Likewise, policies set in a parent domain do not automatically apply to child domains.

The following operations occur when a child domain is created in an existing tree:

- Verification of the name provided as a valid child domain name.
- Location of a source Domain Controller in the parent domain and synchronization of the system time of the child domain with the system time of the source Domain Controller.
- Creation of parent-child TDOs in the System folder on both the parent domain and the child domain. The TDO objects identify two-way transitive trust relationships between the child domain and the parent domain.
- Replication of the Active Directory Schema container and the Configuration container from a domain controller in the parent domain.

Trust Relationships

Active Directory provides security across multiple domains through intra-forest trust relationships. When there are trust relationships between domains in the same forest, the authentication mechanism for each domain trusts the authentication mechanism for all other trusted domains. If a user or application is authenticated by one domain, its authentication is accepted by all other domains that trust the authenticating domain. Users in a trusted domain have access to resources in the trusting domain, subject to the access controls that are applied in the trusting domain.

> **Note:** Default intra-forest trust relationships are created at the time the domains are created. The number of trust relationships required to connect n domains is n–1, whether the domains are linked in a single, contiguous parent-child hierarchy or constitute two or more separate contiguous parent-child hierarchies.

A trust relationship is a relationship established between two domains that allows users in one domain to be recognized by a domain controller in the other domain. Trusts let users access resources in the other domain, and also let administrators manage user rights for users in the other domain. Account authentication between domains is enabled by two-way, transitive trust relationships. All domain trusts in an Active Directory forest are two-way and transitive by default and are have the following attributes:

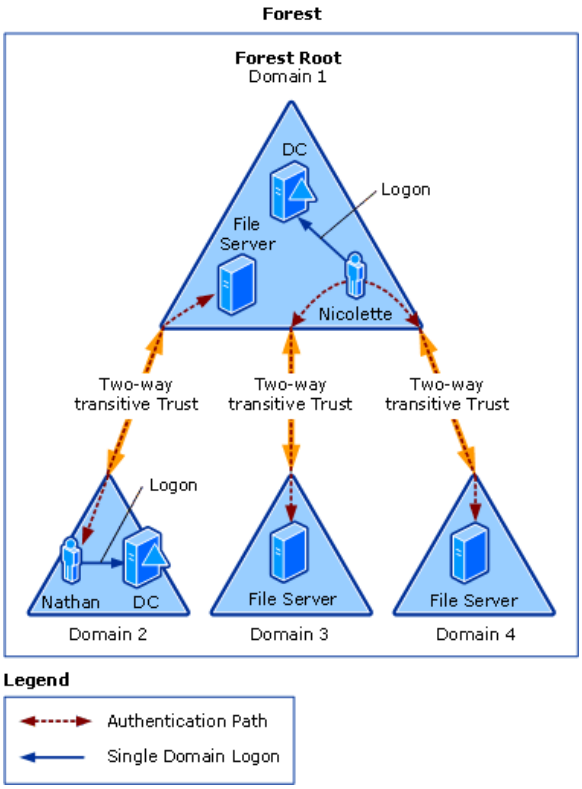
- **Two-way**. When a new child domain is created, the child domain automatically trusts the parent domain, and vice versa. At the practical level, this means that authentication requests can be passed between the two domains in both directions.
- **Transitive**. A transitive trust reaches beyond the two domains in the initial trust relationship. For example, if Domain A and Domain B (parent and child) trust each other, and if Domain B and Domain

Copyright © 2008 Microsoft Corporation.

All rights reserved.

C (also parent and child) trust each other, Domain A and Domain C also trust each other (implicitly), even though no direct trust relationship between them exists.

At the level of the forest, a trust relationship is created automatically between the forest root domain and the root domain of each domain tree added to the forest, with the result that complete trust exists between all domains in an Active Directory forest. At the practical level, because trust relationships are transitive, a single logon process lets the system authenticate a user (or computer) in any domain in the forest. As shown in the following figure, this single logon process lets the account access resources on any domain in the forest.



Note: Single logons enabled by trusts do not necessarily imply that the authenticated user has rights and permissions in all domains in the forest. This is because in any discussion of trust relationships, access to resources always assumes the limitations of access control.

Managing Domains and Trusts

The following subsections provide standard procedures for managing Windows Server 2003 domains and trusts. When joining a Windows Server 2003 domain to a Windows Server 2003 domain forest, a trust relationship is established automatically. As stated earlier, this trust relationship is a two-way, transitive trust relationship. No administrative tasks are required to establish this trust relationship.

Trust relationships within a domain forest are established at the time that the domain is created. Once established, these trust relationships do not need to be managed. Exceptions to this are trust relationships between Windows Server 2003 forests, which require explicit trusts. Explicit trusts are trust relationships that are manually created by administrators, as opposed to trusts created automatically during installation of a Domain Controller.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

DNS configuration and Active Directory

By default, the **Configure Your Server Wizard** and the **Active Directory Installation Wizard** attempt to locate an authoritative DNS server that hosts a primary or secondary copy of a DNS zone for the new domain from its list of configured DNS servers that will accept a dynamic update or a service resource record. If found, all the appropriate records for the Domain Controller are automatically registered with the DNS server after the Domain Controller is restarted.

If a DNS server that can accept dynamic updates is not found, either because the DNS server does not support dynamic updates or dynamic updates are not enabled for the domain, then the Wizard will take the following steps to ensure that the installation process is completed with the necessary registration of the SRV resource records:

- The DNS service is installed on the Domain Controller and is automatically configured with a zone based on the Active Directory domain.

  For example, if the domain chosen for the first domain in the forest is example.microsoft.com, then a zone rooted at the DNS domain name of example.microsoft.com is added and configured to use the DNS Server service on the new Domain Controller.

- A text file containing the appropriate DNS resource records for the Domain Controller is created.

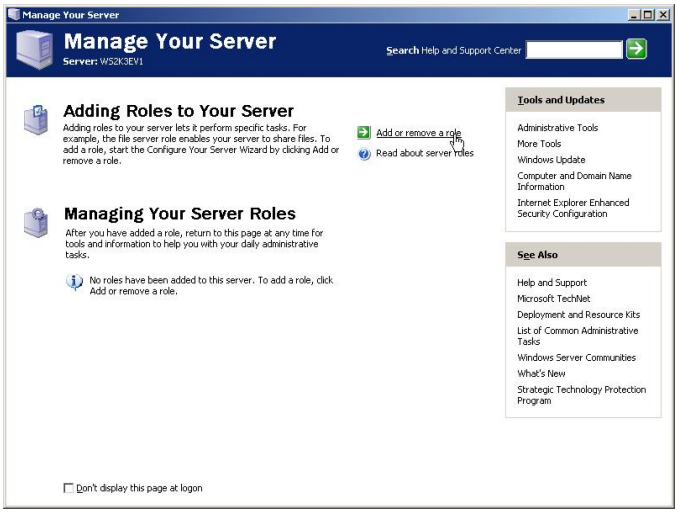
  The file called Netlogon.dns is created in the %systemroot%\System32\Config folder and contains all the records needed to register the resource records of the Domain Controller. Netlogon.dns is used by the Net Logon service and supports Active Directory on servers running non-Windows Server 2003 DNS.

Before running the **Configure Your Server Wizard** or the **Active Directory Installation Wizard**, ensure that the authoritative DNS zone allows dynamic updates and that the DNS server hosting the zone supports the DNS SRV resource record.

Convert a Windows Server 2003 Server to a Domain Controller for a New Forest

To configure the first Domain Controller in a forest after the server installation has been completed, use the following procedures:

1. Log on as an authorized administrator.
2. If the **Manage Your Server** interface is not open, click **Start**, point to **Programs**, point to **Administrative Tools**, and then select on **Manage Your Server**.
3. In the **Adding Roles to Your Server** section, click the **Add or remove a role** link.

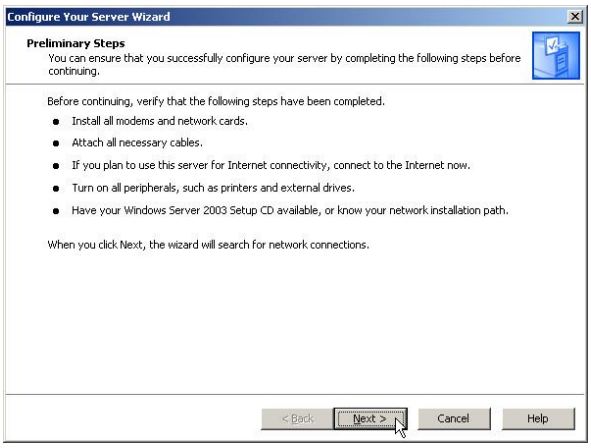


Copyright © 2008 Microsoft Corporation.

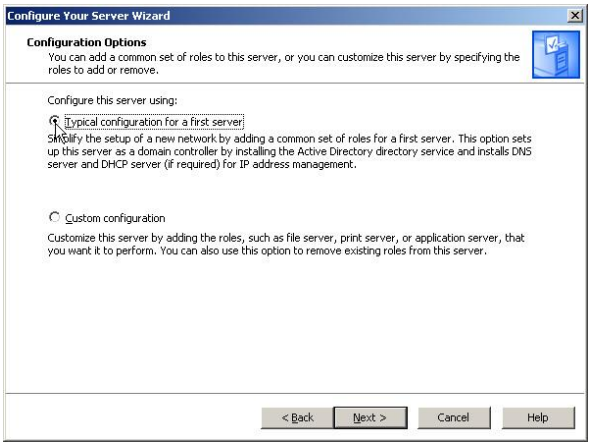
All rights reserved.

Note: Alternatively, the **dcpromo** utility may be used to invoke the **Active Directory Installation Wizard**. The use of **dcpromo** is shown below in the "Create a new domain tree" subsection.

4. The **Configure Your Server Wizard** will appear. Click **Next**.



5. The Wizard will scan the network settings. This may take a few minutes. Once the network settings are determined, the **Configuration Options** page of the Wizard will appear. Select to configure the server as a Domain Controller for a new domain by clicking the **Typical configuration for a first server** radio button.



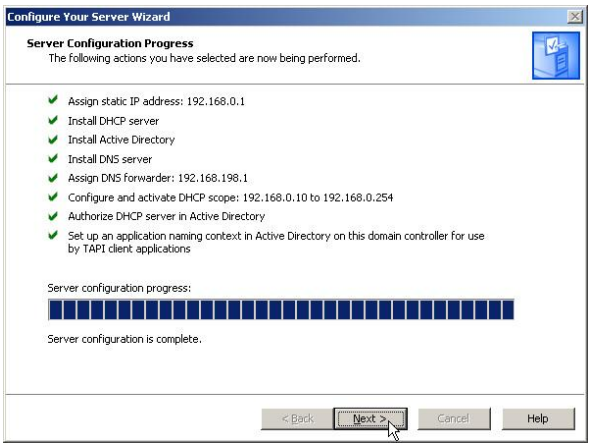
6. Follow all the subsequent instructions from the **Configure Your Server Wizard** to complete the configuration of the first Domain Controller. The Wizard will ask for a DNS name, verification of a Network BIOS (NetBIOS) name, and DNS forwarding requirements.

Note: If the installation CD-ROM is not in the disk drive, a message will appear asking that it be inserted for the configuration process to continue.

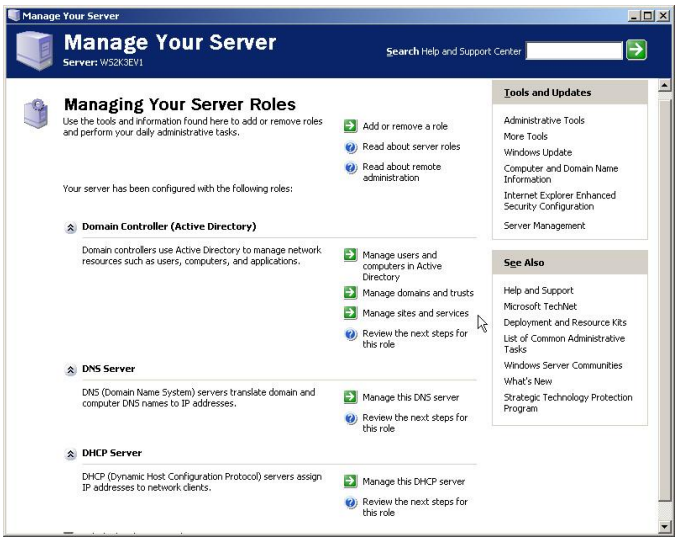
7. When the initial configuration process completes, the server will reboot.
8. Log on to the server as an authorized administrator after it reboots. The **Configure Your Server Wizard** will appear and provide a summary of the actions performed and the services installed. Note that along with Active Directory, a DHCP and DNS server may be installed. Click **Next**, then click **Finish**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



9. The **Manage Your Server** interface will now show the server roles that were installed on the computer and provide options for their management.



Create a New Domain Tree

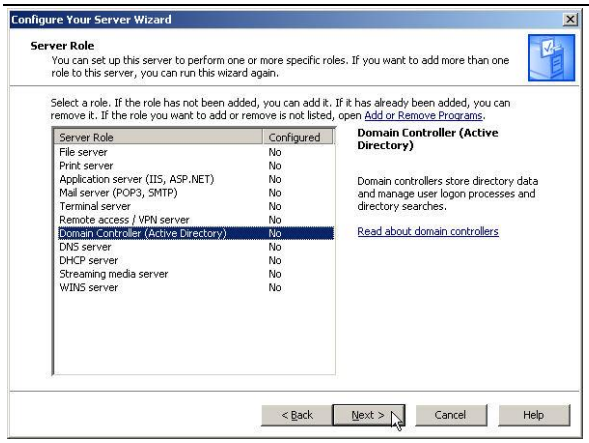
Follow these steps to create a new domain tree:

1. Click **Start**, click **Run**, and then type **dcpromo** to start the **Active Directory Installation Wizard**. Click **Next**.

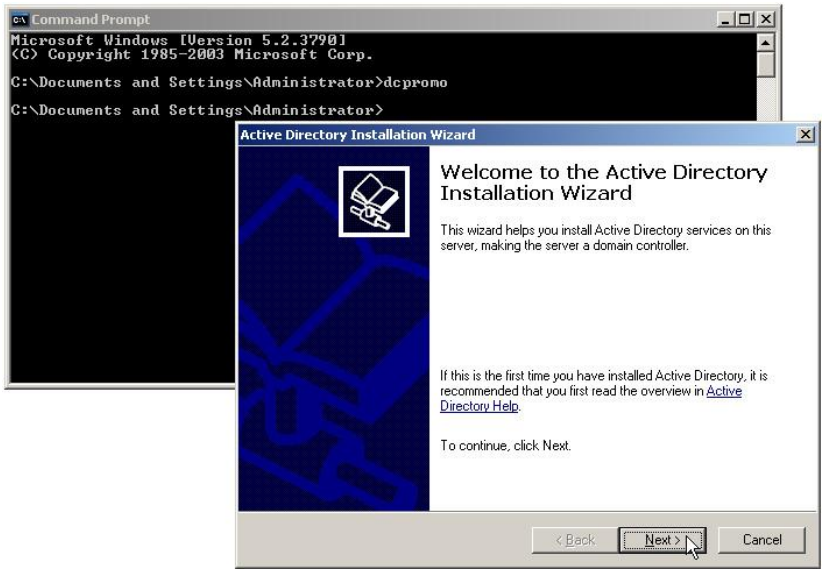
Note: Alternatively, the **Manage Your Server** interface may be used as shown above in the "Convert a Windows Server 2003 server to a Domain Controller for a new forest" subsection.

During the network scan, any existing Domain Controllers will be detected and the **Server Role** page will appear. Select **Domain Controller (Active Directory)** and click **Next** twice.

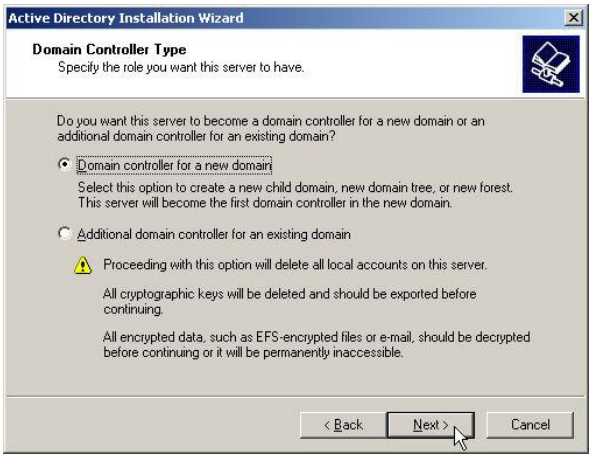
Copyright © 2008 Microsoft Corporation.
All rights reserved.



The **Active Directory Installation Wizard** will be invoked. From that point, the procedures will be the same as those described below.

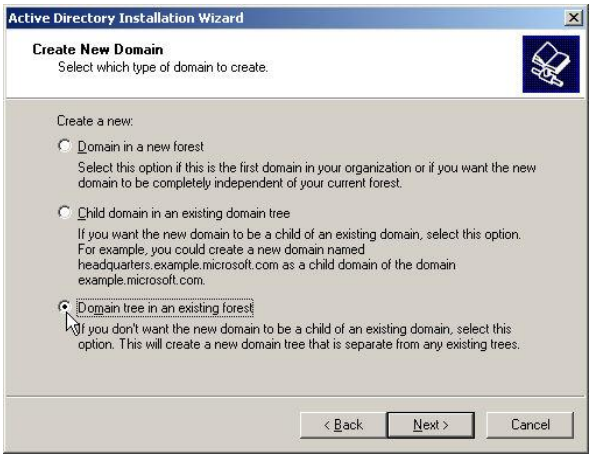


2. On the **Operating System Compatibility** page, read the information and then click **Next**.
3. On the **Domain Controller Type** page, click **Domain controller for a new domain**, and then click **Next**.

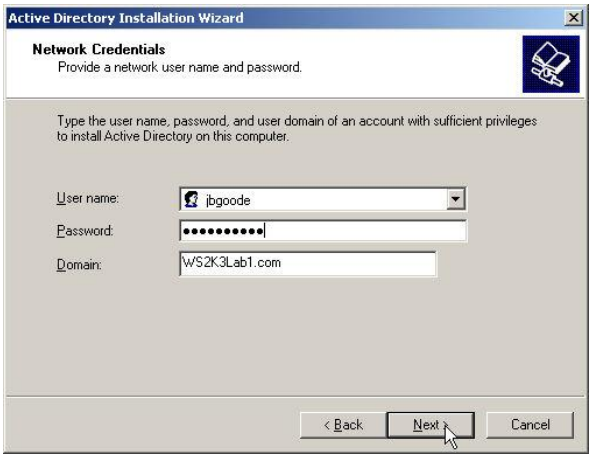


Copyright © 2008 Microsoft Corporation.
All rights reserved.

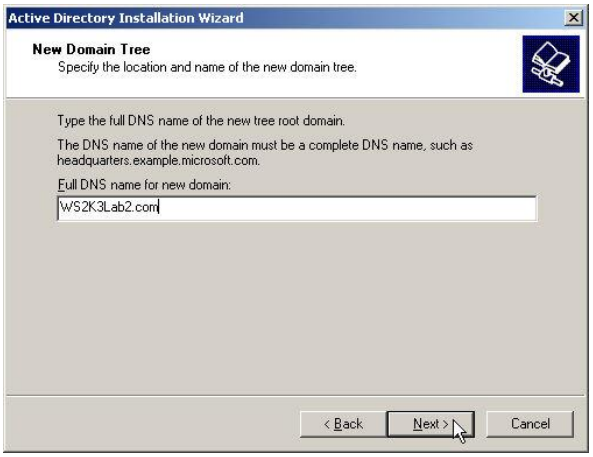
4. On the **Create New Domain** page, click **Domain tree in an existing forest**.



5. On the **Network Credentials** page, type the user name, password, and user domain of the user account to be used for this operation, and then click **Next**. The user account must be a member of the Enterprise Admins group.



6. On the **New Domain Tree** page, type the full DNS name for the new domain, and then click **Next**.



7. On the **NetBIOS Domain Nam**e page, verify the NetBIOS name, and then click **Next**.

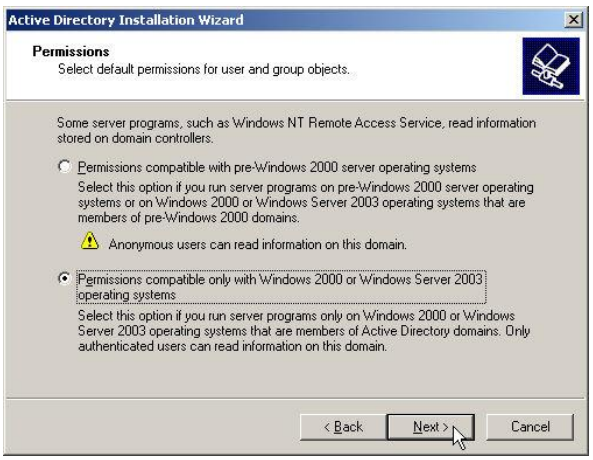
8. On the **Database and Log Folders** page, type the location in which to install the database and log folders, or click **Browse** to choose a location. For this example, accept the defaults and click **Next**.

Copyright © 2008 Microsoft Corporation.

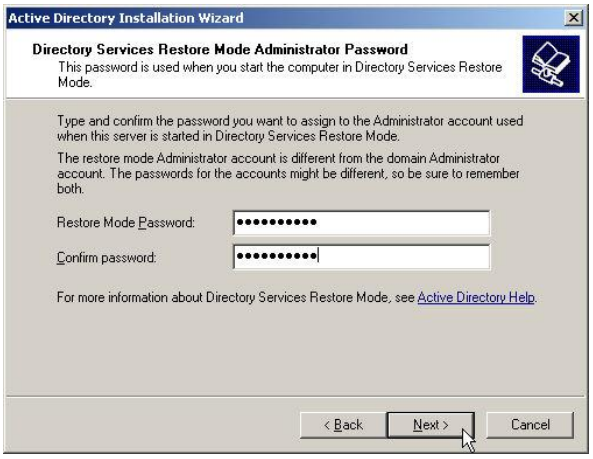
All rights reserved.

9. On the **Shared System Volume** page, type the location in which to install the Sysvol folder, or click **Browse** to choose a location. For this example, accept the defaults and click **Next**.
10. On the **DNS Registration Diagnostics** page, verify if an existing DNS server will be authoritative for this forest or, if necessary, choose to install and configure DNS on this server by clicking **Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server**, and then click **Next**.
11. On the **Permissions** page, select one of the following **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**. Click **Next**.

Note: Permissions compatible with pre-Windows 2000 server operating systems allows anonymous to read information on the domain. Therefore, for the Evaluated Configuration only Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems is used.



12. On the **Directory Services Restore Mode Administrator Password** page, type and confirm the password that is to be assigned to the Administrator account for this server, and then click **Next**. Use this password when starting the computer in Directory Services Restore Mode.



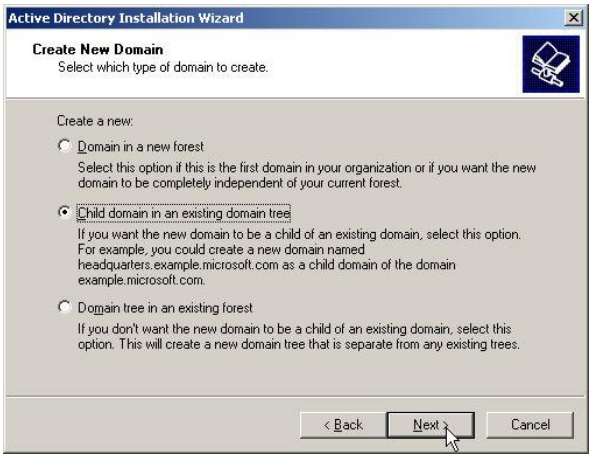
13. Review the **Summary** page, and then click **Next** to begin the installation.
14. In the Completing **the Active Directory Installation Wizard** interface, click **Finish**.
15. Restart the computer.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

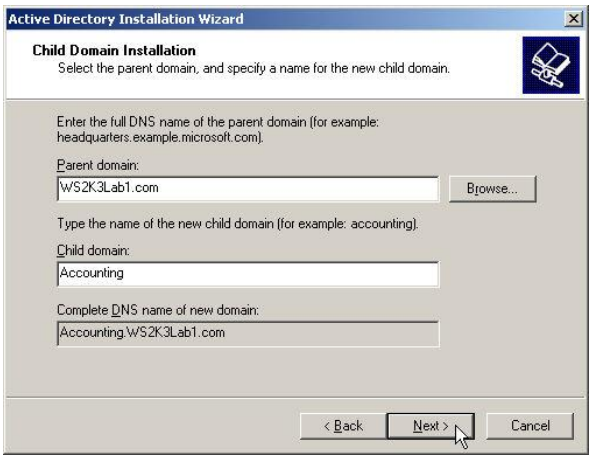
Create a New Child Domain in an Existing Domain Tree

Follow these steps to create a new domain that is to be a child of an existing domain:

1. Click **Start**, click **Run**, and then type **dcpromo** to start the Active Directory Installation Wizard.
2. On the **Operating System Compatibility** page, read the information and then click **Next**.
3. On the **Domain Controller Type** page, click **Domain controller for a new domain**, and then click **Next**.
4. On the **Create New Domain** page, click **Child domain in an existing domain tree**, and then click **Next**.



5. On the **Network Credentials** page, type the user name, password, and user domain of the user account that is to be used for this operation, and then click **Next**. The user account must be a member of the Enterprise Admins group.
6. On the **Child Domain Installation** page, verify the parent domain and type the new child domain name, and then click **Next**.

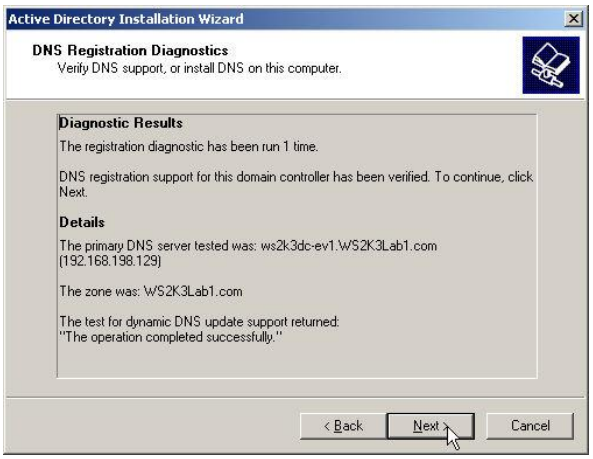


7. On the **NetBIOS Domain Name** page, verify the NetBIOS name, and click **Next**.
8. On the **Database and Log Folders** page, type the location in which to install the database and log folders, or click **Browse** to choose a location. For this example, accept the defaults and click **Next**.
9. On the **Shared System Volume** page, type the location in which to install the Sysvol folder, or click **Browse** to choose a location. For this example, accept the defaults and click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

10. On the **DNS Registration Diagnostics** page, verify the DNS configuration settings are accurate, and then click **Next**.



11. On the **Permissions** page, select one of the following **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems**. Click **Next**.

Note: Permissions compatible with pre-Windows 2000 server operating systems allows anonymous to read information on the domain. Therefore, for the Evaluated Configuration only Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems is used.

12. On the **Directory Services Restore Mode Administrator Password** page, type and confirm the password that is to be assigned to the Administrator account for this server, and then click **Next**. Use this password when starting the computer in Directory Services Restore Mode.
13. Review the **Summary** page, and then click **Next** to begin the installation.
14. In the **Completing the Active Directory Installation Wizard** interface, click **Finish**.
15. Restart the computer.

Add a Domain Controller to an Existing Domain

After creating multiple Domain Controllers, the Active Directory will automatically replicate directory information between them. If a Domain Controller becomes unavailable, directory information is still available through the other Domain Controllers.

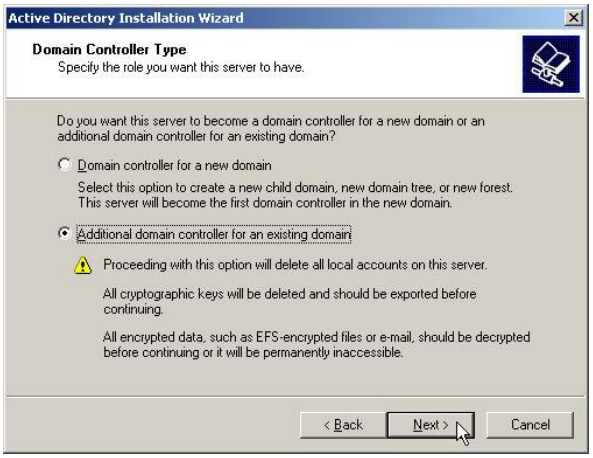
Follow these steps to add an additional Domain Controller to an existing domain:

1. Click **Start**, click **Run**, and then type **dcpromo /adv** to open the Active Directory Installation Wizard with the option to create an additional Domain Controller from restored backup files.

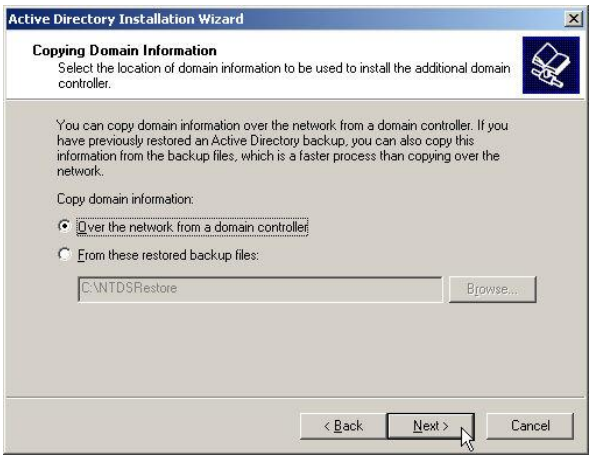
Note: The use of **dcpromo** with the **/adv** switch is being used here as an example. The **/adv** switch is only necessary when it is desired to create a Domain Controller from restored backup files. It is not required when creating an additional Domain Controller over the network.

2. On the **Operating System Compatibility** page, read the information and then click **Next**.
3. On the **Domain Controller Type** page, click **Additional Domain Controller for an existing domain**, and then click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

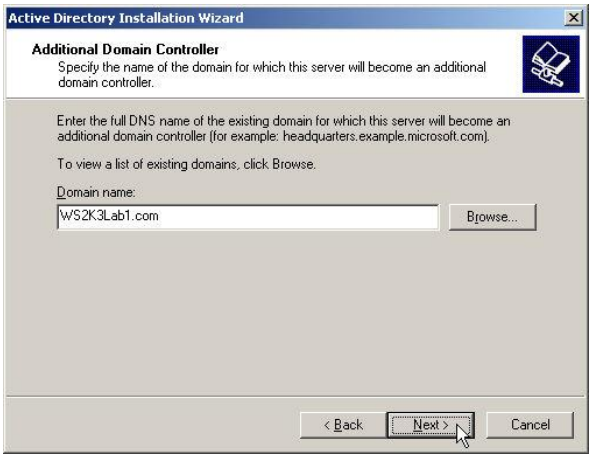


4. On the **Copying Domain Information** page, select from the following:
   - **Over the network from a Domain Controller**.
   - **From these restored backup files**.
5. For this example, click the **Over the network from a Domain Controller** radio button and click **Next**.

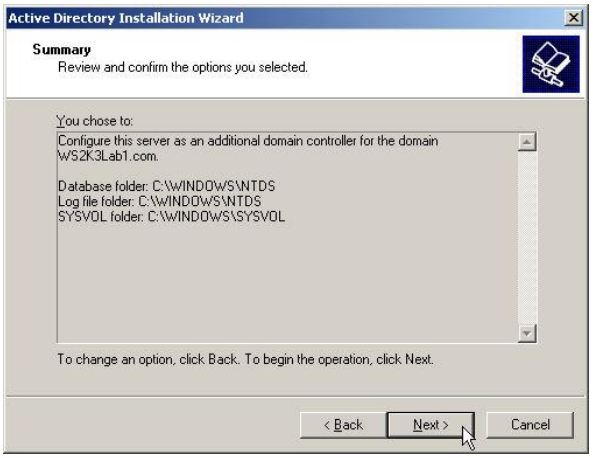


6. On the **Network Credentials** page, type the user name, password, and user domain of the user account that will be used for this operation, and then click **Next**. The user account must be a member of the Domain Admins group for the target domain.
7. Enter the full DNS name of the existing domain for which this server will become an additional Domain Controller. Click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



8. On the **Database and Log Folders** page, type the location where the database and log folders are to be installed, or click **Browse** to choose a location, and then click **Next**.
9. On the **Shared System Volume** page, type the location the Sysvol folder is to be installed, or click **Browse** to choose a location, and then click **Next**.
10. On the **Directory Services Restore Mode Administrator Password** page, type and confirm the password that that is to be assigned to the Administrator account for this server, and then click **Next**. Use this password when starting the computer in Directory Services Restore Mode.
11. Review the **Summary** page, and then click **Next** to begin the installation.



12. In the **Completing the Active Directory Installation Wizard** interface, click **Finish**.
13. Restart the computer.

Raise the Domain Functional Level

Functional levels are an extension of the mixed/native mode concept introduced in Microsoft Windows 2000 to activate new Active Directory features after all the domain controllers in the domain or forest are running the Windows Server 2003 operating system. When a computer that is running Windows Server 2003 is installed and promoted to a Domain Controller, new Active Directory features are activated by the Windows Server 2003 operating system over its Windows 2000 counterparts. Additional Active Directory features are available when all Domain Controllers in a domain or forest are running Windows Server 2003 and the administrator activates the corresponding functional level in the domain or forest.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

To activate the new domain features, all Domain Controllers in the domain must be running Windows Server 2003. After this requirement is met, the administrator can raise the domain functional level to Windows Server 2003.

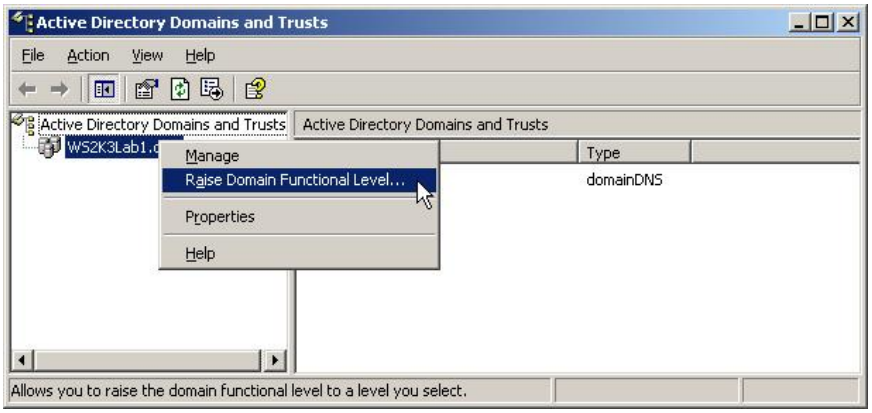
To activate new forest-wide features for Windows Server 2003, all Domain Controllers in the forest must be running Windows Server 2003, and their current domain functional level must be at Windows Server 2003 domain level. After this requirement is met, the administrator can raise the forest functional level.

Network clients can authenticate or access resources in the domain or forest without being affected by the Windows Server 2003 domain or forest functional levels. These levels only affect the way that Domain Controllers interact with each other.

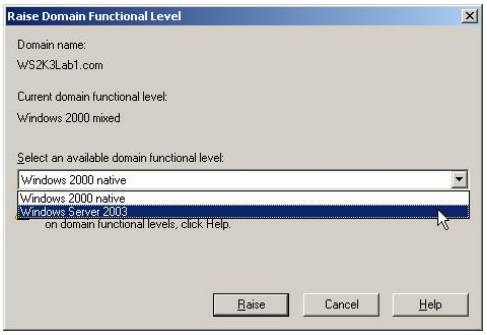
Note: The Evaluated Configuration uses only Server 2003 domains.

To raise the domain functional level:

1. Log on as a member of the Domain Admins group.
2. Open **Active Directory Domains and Trusts**.
3. In the console tree, right-click the domain for which the functionality is to be raised, and then select **Raise Domain Functional Level**.



4. In **Select an available domain functional level**, do one of the following:
   - To raise the domain functional level to Windows 2000 native, click **Windows 2000 native**, and then click **Raise**.
   - To raise domain functional level to Windows Server 2003, click **Windows Server 2003**, and then click **Raise**.



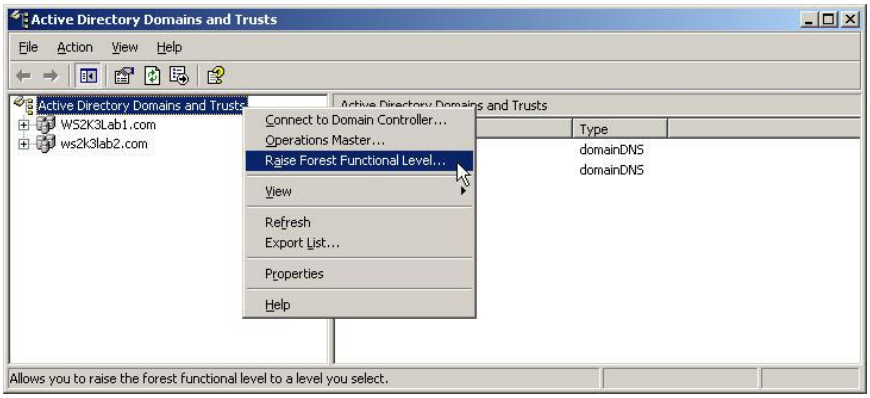
Note: The domain functional level can also be raised by right-clicking a domain displayed in Active Directory Users and Computers, and then selecting **Raise Domain Functional Level**.

Copyright © 2008 Microsoft Corporation.

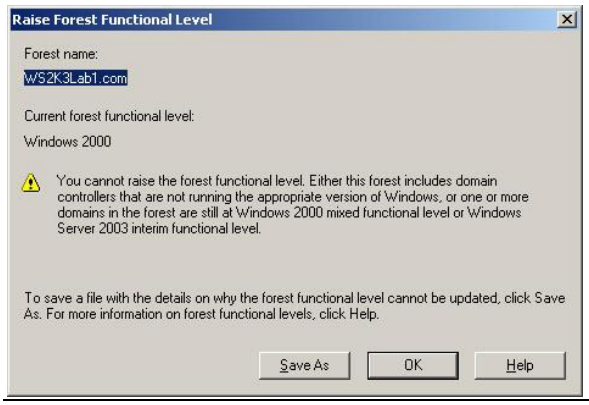
All rights reserved.

To raise the forest functional level:

1. Log on to the forest root domain as a member of the Enterprise Admins group.
2. Open **Active Directory Domains and Trusts**.
3. In the console tree, right-click the **Active Directory Domains and Trusts** node, and then select **Raise Forest Functional Level**.

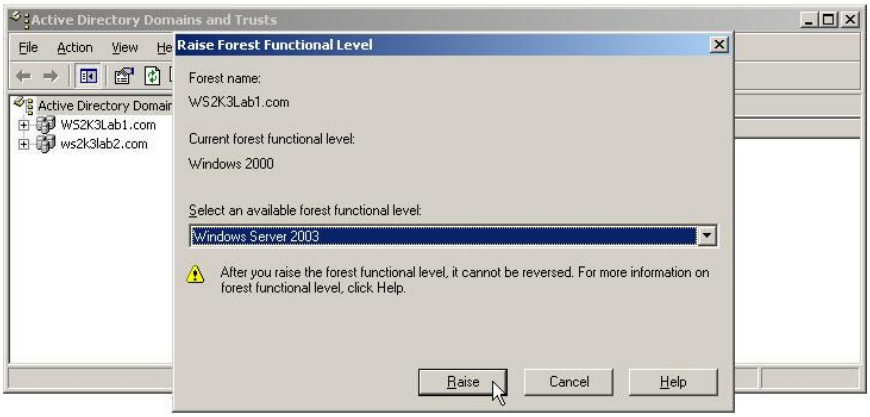


Note: The forest functional level cannot be raised until all domain in the forests are at Windows Server 2003 functional level. If domains are detected at a lower functional level the message below will appear. By clicking Save As, a file can be created that identifies all of the domains that are not at the proper functional level. Make the necessary functional level upgrades before proceeding.



4. If all domains in the forest are at the **Windows Server 2003** functional level, the **Raise Forest Functional Level** interface shown below will appear. The only available option will be **Windows Server 2003**. Click **Raise**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. A warning message will appear. Click **OK**.

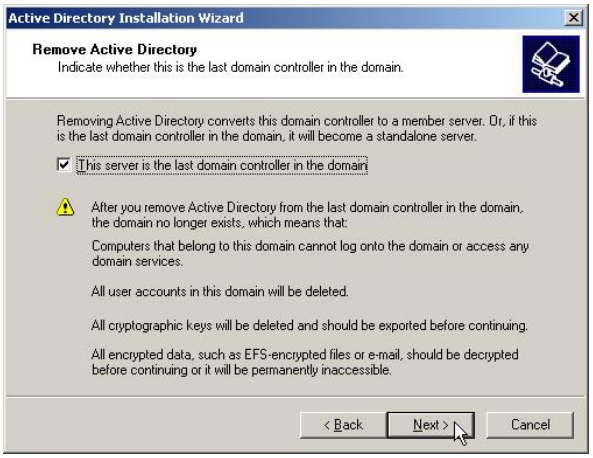
6. A confirmation message will appear. Click **OK**.

Remove a Domain

1. On the last Domain Controller in the domain, click **Start**, and then click **Run**.
2. In **Open**, type **dcpromo** to open the **Active Directory Installation Wizard**, and then click **Next**.
3. A warning message may appear indicating that this Domain Controller is a Global Catalog server. Read the message and take appropriate action if necessary. Click **OK**.

4. On the **Remove Active Directory** page, select the **This server is the last Domain Controller in the domain** check box, and then click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. Continue to follow instruction in the Wizard to remove the domain.

Warning: Removing a domain will result in the permanent loss of any data contained in that domain. This includes all user, group, and computer accounts.

Configuring One-way Non-transitive Trusts

Explicit trusts are trust relationships that are created by administrators, as opposed to trusts created automatically during installation of a Domain Controller. Explicit trusts are created and managed using **Active Directory Domains and Trusts**.

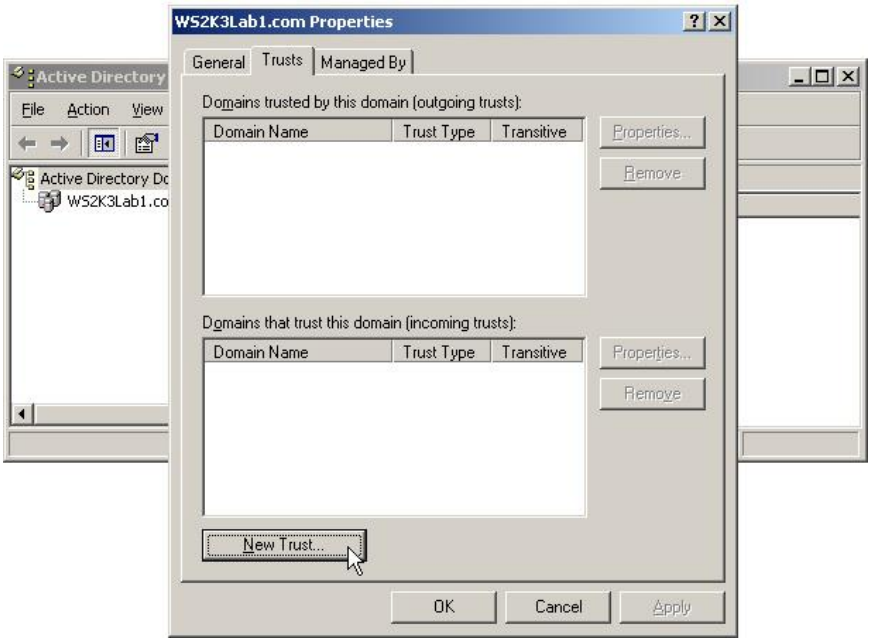
There may be times when explicit trust relationships need to be created between domains. One example is when domains in disparate forests need to trust one another. An administrator of a domain can accomplish this by setting up a non-transitive, or one-way, trust with another domain. A non-transitive trust is bounded by the two domains in the trust relationship and does not flow to any other domains in the forest. Remember that the trust being established makes a domain the "trusting" domain. That means that another domain is being chosen to trust. It does not mean that the other domain will agree with the trust. (The administrator of the other domain has to follow the same procedures.)

Follow these steps to initiate a one-way trust:

1. From a Domain Controller on the trusted domain, start the **Active Directory Domains and Trusts** snap-in.
2. In the console tree, right-click the domain node for the forest root domain, and then click **Properties**.
3. On the **Trust** tab, click **New Trust**.

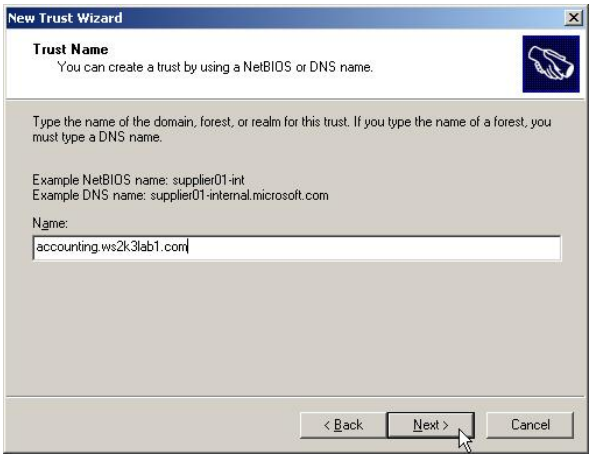
Copyright © 2008 Microsoft Corporation.

All rights reserved.



4. Click **Next** on the **New Trust Wizard**.

5. On the **Trust Name** page, type the DNS name of another forest, and then click **Next**.



6. On the **Trust Type** page, click **Forest trust**, and then click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

7. On the **Direction of Trust** page, select one of the following:
   - To create a two-way, forest trust, click **Two-way**. Users in this forest and users in the specified forest can access resources in either forest.
   - To create a one-way, incoming forest trust, click **One-way:incoming**. Users in the specified forest will not be able to access any resources in this forest.
   - To create a one-way, outgoing forest trust, click **One-way:outgoing**. Users in this forest will not be able to access any resources in the specified forest.
8. For this example, click **One-way:outgoing**. Click **Next** and continue to follow the Wizard.

Note: To selectively limit authentication to particular users and groups from the specified forest, on the **Outgoing Trust Properties** page, click **Selective authentication**. This option is preferred if the specified forest belongs to a separate organization.

9. Log on to a Domain Controller in the trusting domain, start the **Active Directory Domains and Trusts** interface.
10. Follow the same procedures as above to open the **New Trust Wizard**.
11. On the **Direction of Trust** page, select **One-way:incoming**. Click **Next** and continue to follow the Wizard.

Smart Card Deployment

Most organizations use passwords to manage access to computer networks and resources. However, some users set weak passwords, write passwords down in insecure locations, or forget their passwords and require help desk assistance for password reset. For this reason, passwords alone might not provide the level of security and manageability that an organization requires.

Smart card support in Microsoft Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition operating systems provides users with stronger credentials than even the most complex passwords. If smart cards are used, managed, and deployed properly, they can enhance the security of an organization and reduce support costs.

Smart cards offer the following benefits:

- **Protection**. Smart cards provide tamper-resistant storage for private keys and other data. If a smart card is lost or stolen, it is difficult for anyone except the intended user to use the credentials that it stores.
- **Isolation**. Cryptographic operations are performed on the smart card itself rather than on the client or on a network server. This isolates security-sensitive data and processes from other parts of the system.
- **Portability**. Credentials and other private information stored on smart cards can easily be transported between computers at work, home, or other remote locations.

The number and variety of smart card-enabled applications is growing to meet the needs of organizations that want to rely on smart cards to enable secure authentication and to facilitate services.

Before deploying smart cards, a public key infrastructure (PKI) must be in place. Next, applications that will be enabled for use with smart cards need to be identified, and there needs to be a plan in place on how the organization is going to implement and support a smart card infrastructure.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Supported Smart Card Reader and Smart Card for the Evaluated Configuration

Only the Smart Card components listed below are allowed for use in the Windows Server 2003 Evaluated Configuration.

Smart Card Reader Manufacturer	Smart Card Reader	Interface	Device Driver
Gemplus	GemPC Twin	USB	Usbccid.sys

Smart Card Manufacturer	Default PIN	CSP
Infineon Technologies	12345678	Microsoft Base Smart Card Crypto Provider

Installing a Smart Card Reader

Note: To avoid the need to point the **%SystemRoot%\INF-Temp** folder created during the Evaluated Configuration process and the **%SystemDirectory%\drivers** folder, as defined in the procedures below, temporarily take the system out of the Evaluated Configuration by moving the .inf files to their default location. After installing the Smart Card reader, the .inf files will need to be moved again, following the procedures in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* in order to remain compliant with the Evaluated Configuration. Otherwise, follow the procedures below and point the Found New Hardware Wizard to the new file locations as indicated.

1. Depending on the type of Smart Card reader purchased, attach the reader to an available Universal Serial Bus (USB) port. The Evaluated Configuration of Windows Server 2003 disables the ability of the smart card reader to be installed automatically because the system will not be able to find the driver in its default location.

   Note: The Smart Card reader for the Evaluated Configuration uses a USB port. The proper driver for the Evaluated Configuration is **Version 5.2.3790.1830**, which is found on a default installation of Windows Server 2003 with SP1 or higher.

2. The Plug and Play service will try to find the device drivers by searching the **%SystemRoot%\inf** folder for a driver reference. It will not be able to find a driver reference and as a result, the **Found New Hardware Wizard** will appear. Select the **No, not at this time** radio button and click **Next**.

3. Select the **Install from a list or specific location (Advanced)** radio button and click **Next**.

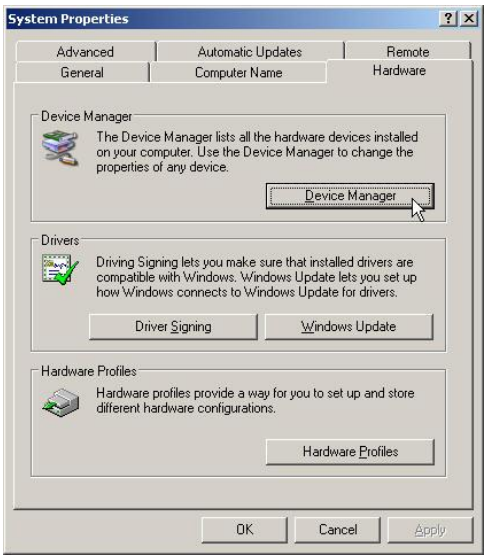
Copyright © 2008 Microsoft Corporation.
All rights reserved.

4. Uncheck the **Search removable media (floppy, CD-ROM…)** check box and check the **Include this location in the search** check box.
5. Enter the path to the **%SystemRoot%\INF-Temp** folder created when the operating system was configured, or click the **Browse** button to find and select the **%SystemRoot%\INF-Temp** folder. Click **Next**.

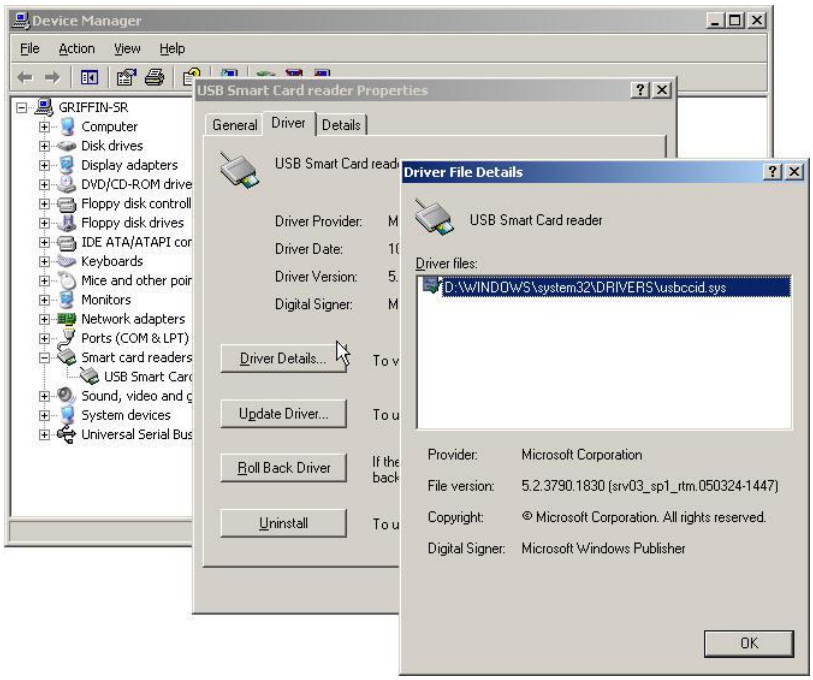
6. The **Found New Hardware Wizard** will search the **%SystemRoot%\INF-Temp** folder for an INF file containing a driver reference. Once the file is found, a message may appear indicating that the driver has not passed Windows Logo testing. This occurs because the .inf files were moved from their default location and the Plug and Play service cannot find the matching Windows Logo certificate. Click **Continue Anyways**.

7. The **Files Needed** interface may appear, asking for the location of the driver files. Enter the path to the **%SystemDirectory%\drivers** folder or click the **Browse** button to find and select the **%SystemDirectory%\drivers** folder. Click **OK**.
8. The **Found New Hardware Wizard** interface will indicate when the driver installation is finished. Click **Finish** to close the Wizard.
9. If desired, verify that the proper installation of the Smart Card reader. Click **Start**, right-click on My Computer, and select **Properties**.
10. In the **System Properties** interface, click the **Hardware** tab then click the **Device Manager** button.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



11. In the **Device Manager** interface, expand **Smart card readers**, then right-click **USB Smart Card reader** and select **Properties**.
12. Click the **Driver details** button in the **Smart Card reader Properties** interface and verify that the **Usbccid.sys** driver is used.



13. Close all the interfaces.

Smart Card Certificate Enrollment

A domain user cannot enroll for a Smart Card Logon certificate (which provides authentication) or a Smart Card User certificate (which provides authentication plus other uses of the smart card cryptography) unless a system administrator has granted the user access rights to the Certificate Template that is stored in Active Directory. Enrollment for a smart card certificate must be a controlled procedure, in the same manner that employee badges are controlled for purposes of identification and physical access. The

Copyright © 2008 Microsoft Corporation.

All rights reserved.

recommended method for enrolling users for smart card-based certificates and keys is through a dedicated smart card enrollment station.

A smart card enrollment station is used by a designated Smart Card Enrollment Agent to act on behalf of a user to request and install a Smart Card Logon certificate or Smart Card User certificate on the user's Smart Card. Prior to using the Smart Card Enrollment station, the smart card issuer must have obtained a signing certificate based on the Enrollment Agent certificate template. The signing certificate signs the certificate request that is generated on behalf of the smart card recipient.

By default, only domain administrators are granted permission to request a certificate based on the Enrollment Agent template. A user other than a domain administrator can be granted permission to enroll for an Enrollment Agent certificate by setting permissions for that user on the Enrollment Agent certificate template. Once someone has an Enrollment Agent certificate, they can enroll for a certificate and generate a smart card on behalf of anyone in the organization. The resulting smart card could then be used to log on to the network and impersonate the real user.

Note: For the Evaluated Configuration, Enrollment Agent certificates must only be granted to accounts that are assigned to the Certificate Manager role as defined in Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide. Procedures for modifying and assigning an Enrollment Agent certificate are demonstrated below.

Because of the powerful capability of the Enrollment Agent certificate, it is strongly recommended that very strong controls are maintained over who has one. A scenario to minimize risk of Enrollment Agent certificate misuse would be to have one subordinate CA with very tight administrative controls in the organization that is only used to issue Enrollment Agent certificates. Once the initial Enrollment Agent certificates have been issued, the administrator of the CA can disable the issuance of Enrollment Agent certificates until they are needed again. By restricting the administrators who can operate the CA service on the subordinate CA, the service can be kept online for the generation and distribution CRLs if necessary. Other CAs in the hierarchy can still issue Enrollment Agent certificates if their policy settings are changed, but authorized administrators can determine whether inappropriate Enrollment Agent certificates are issued by checking the Issued Certificates log for each CA regularly.

Note: For information on how to configure and administer a certification server for the Evaluated Configuration, see Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide, and Appendix B, Windows Server 2003 Certificate Server Evaluated Configuration Administrator's Guide.

The enrollment station does not provide any smart card personalization functions, such as creating a file structure or setting the PIN, because those are card-specific functions and can only be done using specialized software provided by the smart card manufacturer.

Prepare a Certification Authority to Issue Smart Card Certificates

To prepare a CA to issue smart card certificates, first logon to the CA as a member of the Domain Admins group to create duplicates of the Smart Card Logon, Smart Card User, and Enrollment Agent certificate templates and ensure security permissions and ownership are properly set on the templates. After setting the proper permissions and ownership on the templates, log on as the CA administrator to assign the Enrollment Agent role and import the Smart Card templates that will be issued.

Create a duplicate template and grant ownership to the CA Administrator:

Note: The CA Administrator role is defined in Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide for the Evaluated Configuration.

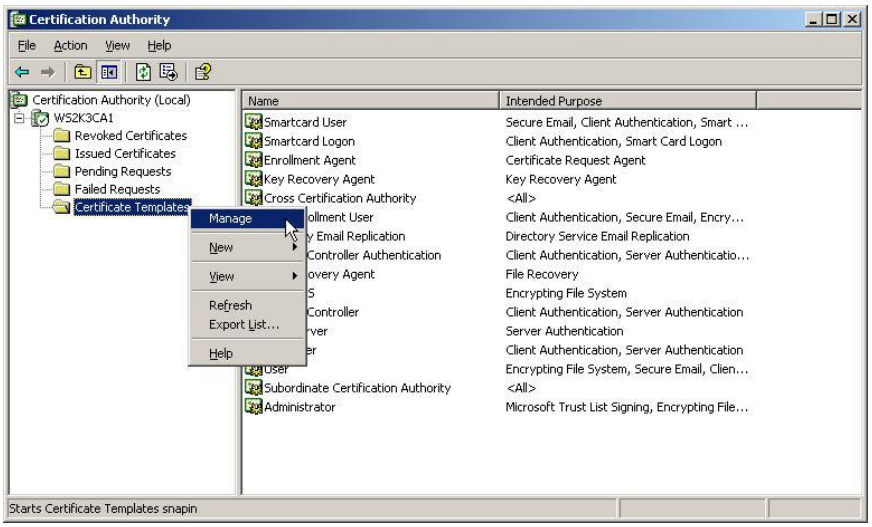
1. Log on with domain administrator rights to the CA used to issue smart card certificates.

Copyright © 2008 Microsoft Corporation.

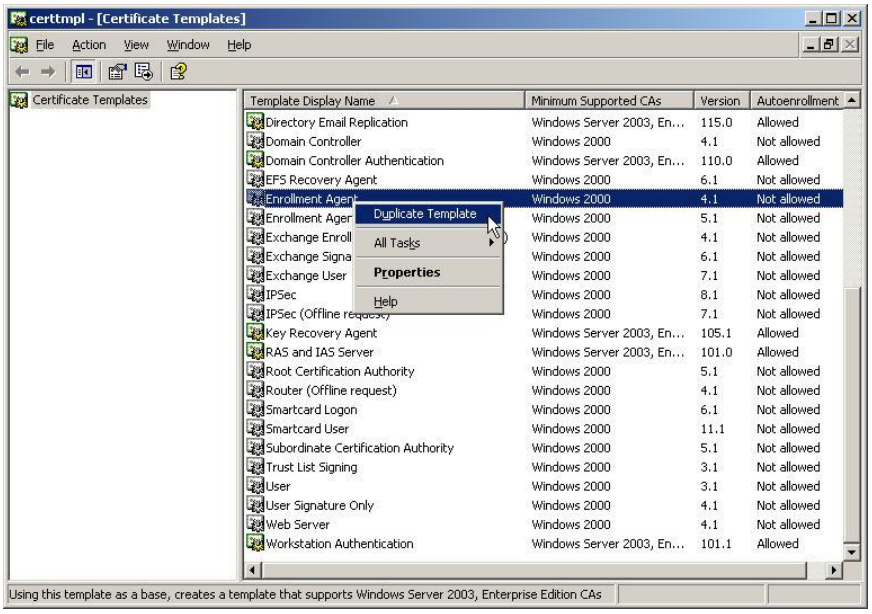
All rights reserved.

2. Open **Certification Authority**. Click **Start**, select **Control Panel**, double-click **Administrative Tools**, and then double-click **Certification Authority**.

3. Expand the CA node then right-click **Certificate Templates** and select **Manage**.

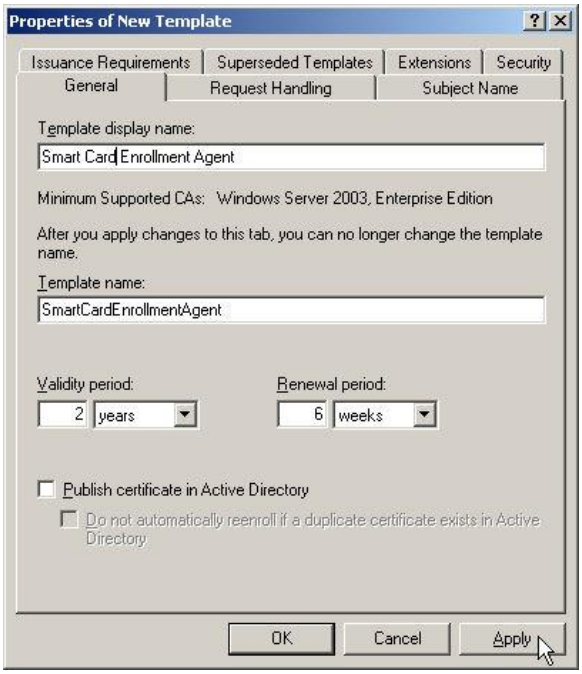


4. In the **Certificate Templates** interface, right-click the **Enrollment Agent** certificate and select **Duplicate Template**.

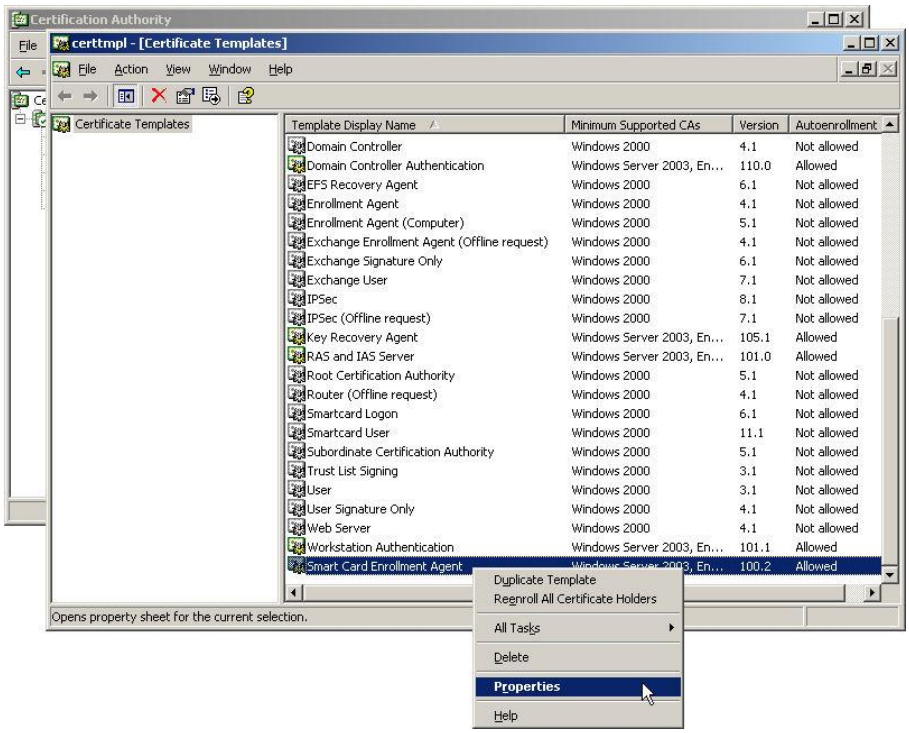


5. Enter a new name for the template, such as **Smart Card Enrollment Agent**. Click **Apply** or **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

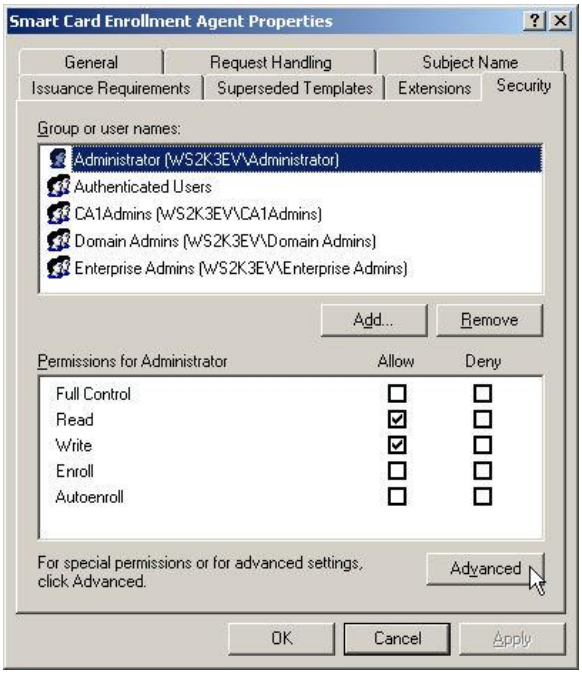


6. Find the new duplicate template in the **Certificate Templates** interface, then right-click on it and select **Properties**.

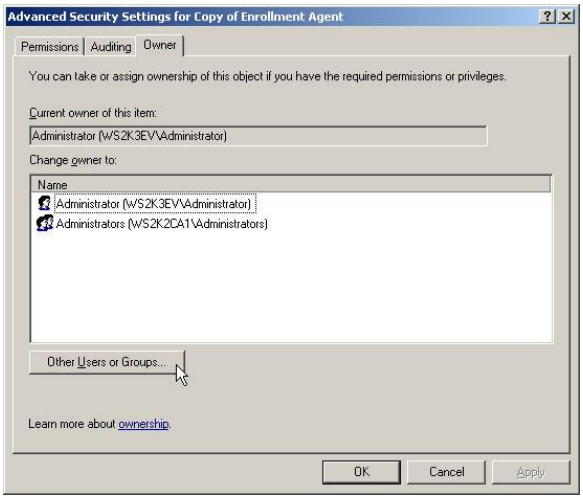


7. Click the **Security** tab of the **Properties** interface and then click the **Advanced** button.

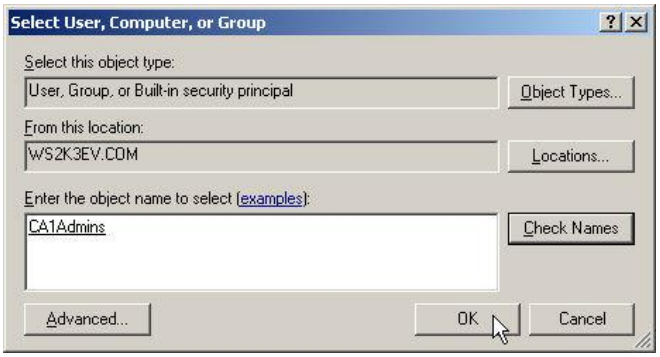
Copyright © 2008 Microsoft Corporation.
All rights reserved.



8. In the **Advanced Security Settings for <name of template>** interface, click the **Owner** tab then click **Other Users or Groups**.

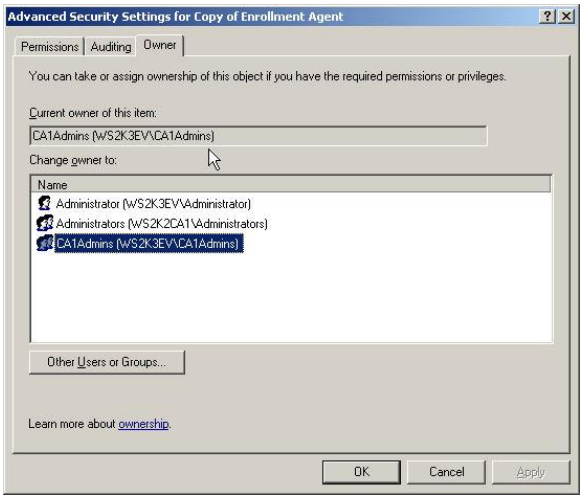


9. Find and enter the appropriate CA administrator's group or user account in the **Select User, Computer, or Group** interface and click **OK**.

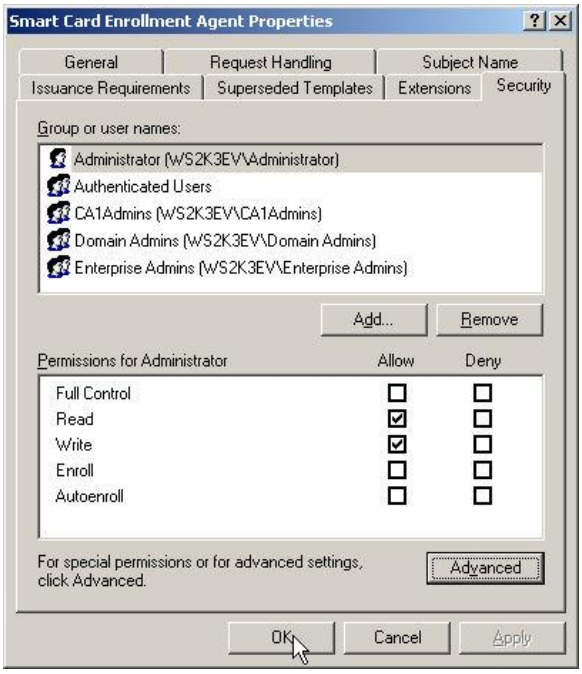


Copyright © 2008 Microsoft Corporation.
All rights reserved.

10. Select the CA administrator account from the **Change owner to** list and click **Apply**. The account will appear in the **Current owner of this item** text box.



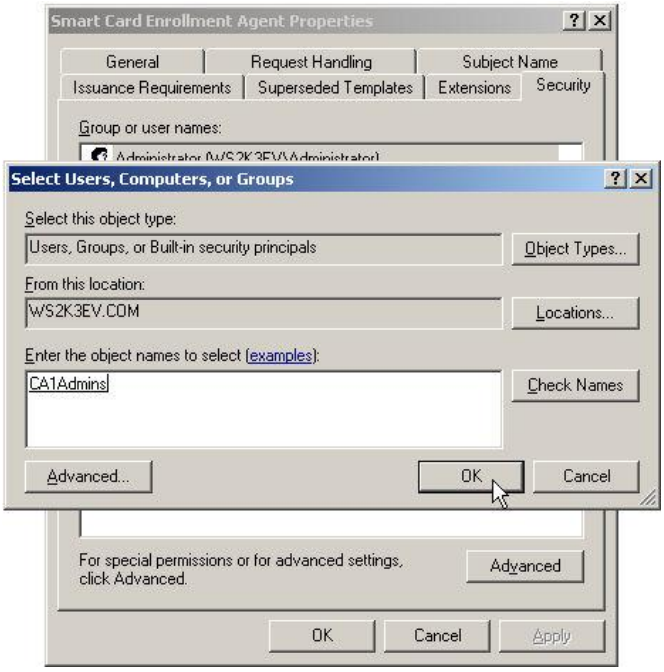
11. Click **OK** to close the **Advanced Security Settings for <name of template>** interface, and close the **Properties** interface by clicking **OK**.



12. If permissions for the CA Administrator are not yet set on the template, click **Add** on the template Properties interface to add CA administrator group or user account permissions to the template. Give the CA Administrator account Full Control permissions to the template.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



13. The Smart Card Enrollment Agent template must only be used by a user that has been designated as an authorized enrollment agent. Therefore, to prevent other users from enrolling for that certificate, select the **Authenticated Users** group in the **Security** tab view of the **Smart Card Enrollment Agent Properties** interface and remove the **Enroll** permission. This will leave the **Authenticated Users** group with **Read** permission to the template.

Note: Step 13 applies only to the Smart Card Enrollment Agent certificate template. The **Enroll** permission for **Authenticated Users** is needed for the **Smart Card Logon** and **Smart Card User** templates.

---

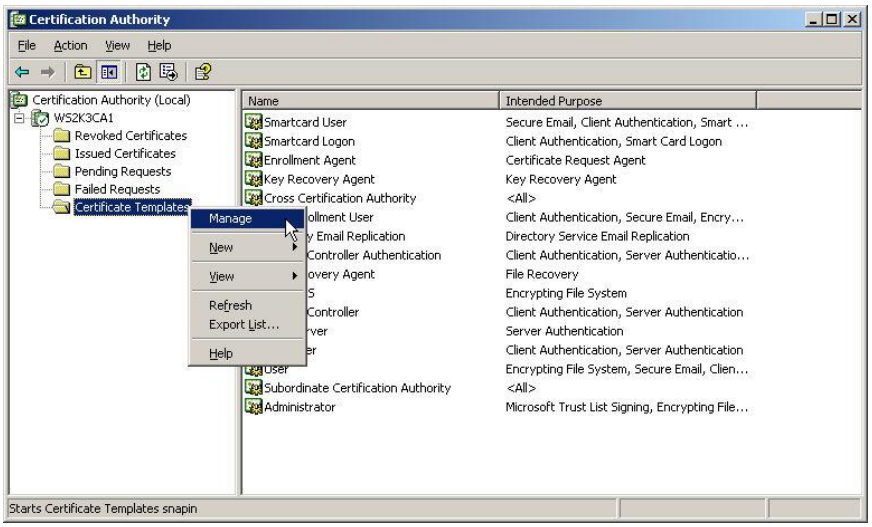
14. Repeat the procedures above for creating duplicate templates and granting ownership to the CA Administrator for the **Smart Card Logon** and **Smart Card User** templates.

Set permissions on certificate template for the designated smart card enrollment agent and Authenticated Users:

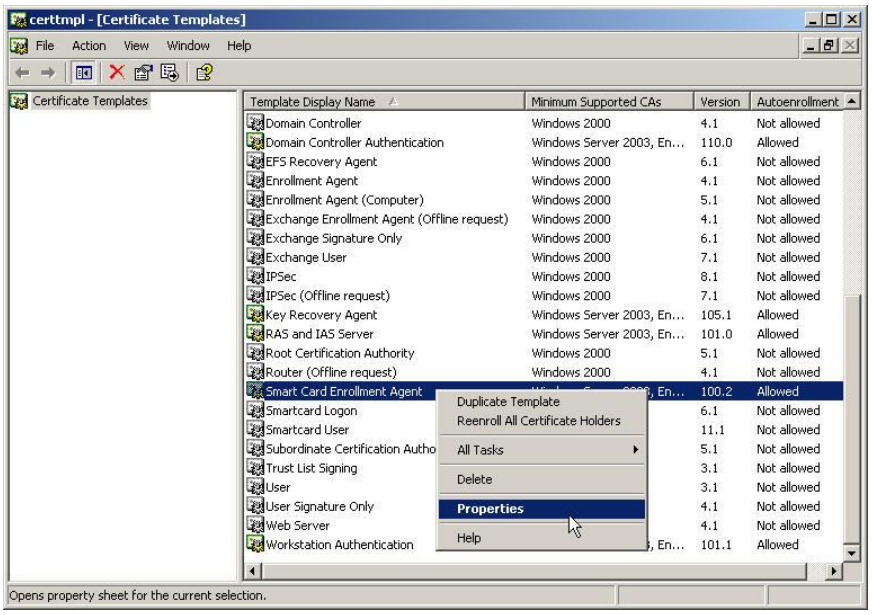
1. Log on as the CA administrator or a domain administrator.
2. Open **Certification Authority**. Click **Start**, select **Control Panel**, double-click **Administrative Tools**, and then double-click **Certification Authority**.
3. Expand the CA node then right-click **Certificate Templates** and select **Manage**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

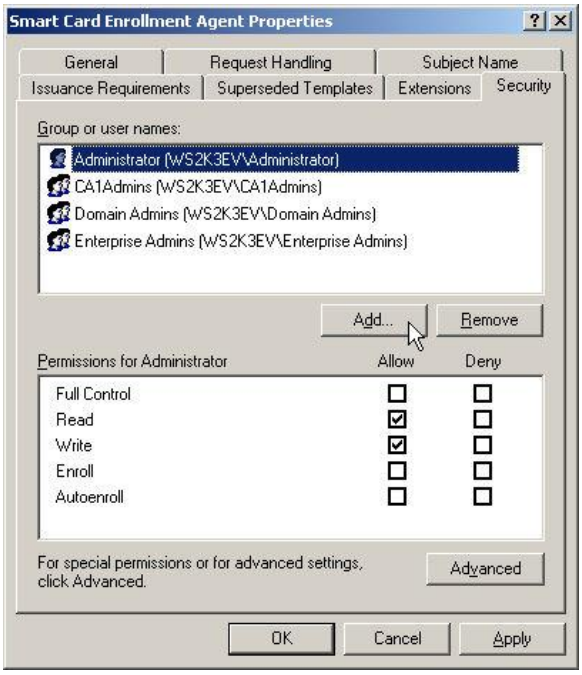


4. In the **Certificate Templates** interface, right-click on the **Smart Card Enrollment Agent** template (copy of **Enrollment Agent** template) and select **Properties**.

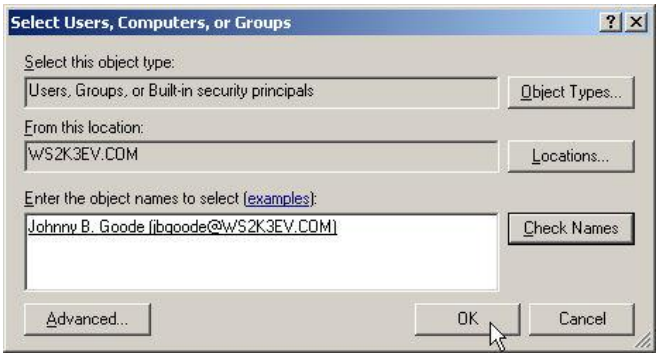


5. Click the **Security** tab on the **Properties** interface then click the **Add** button.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

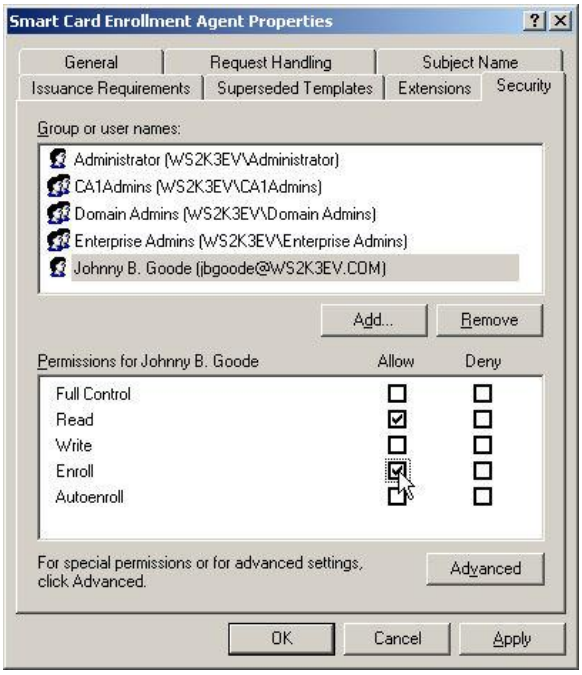


6. Find and enter the appropriate smart card enrollment agent group or designated user account in the **Select User, Computer, or Group** interface and click **OK**.

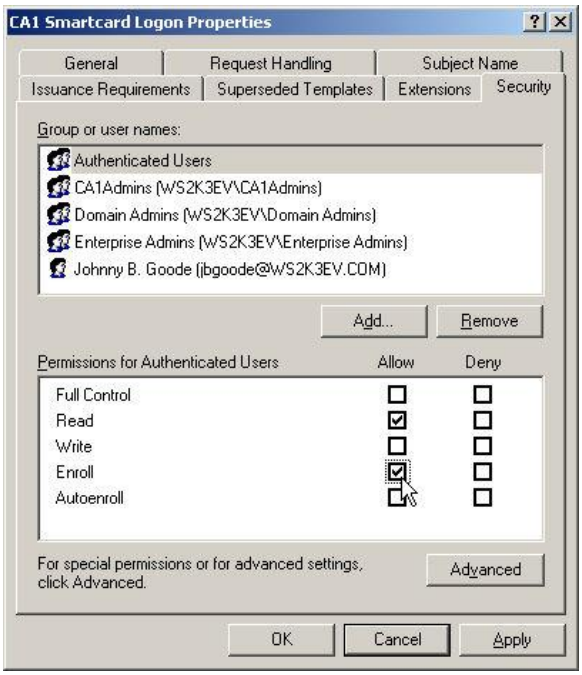


7. Assign the **Read** and **Enroll** permissions to the designated enrollment agent account.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



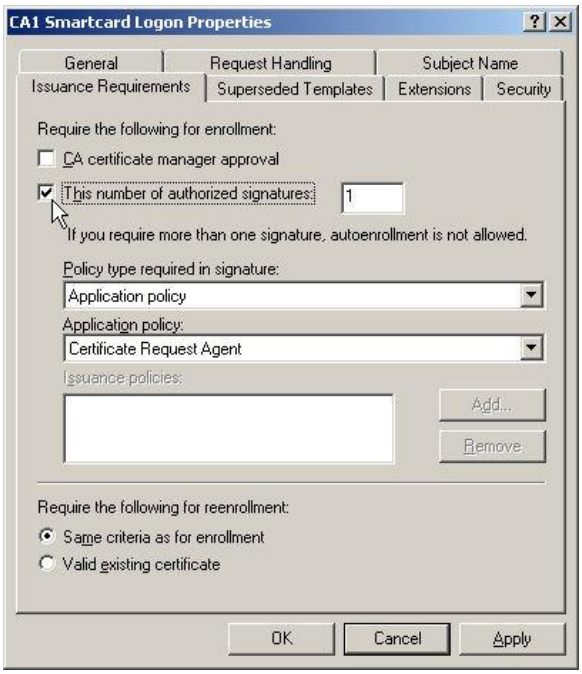
8. Click **OK** to close the **Properties** interface.
9. In the **Certificate Templates** interface, right-click on the **Smart Card Logon** template (**CA1 Smart Card Logon** is the name of the duplicate template used in this example) and select **Properties**.
10. Click the **Security** tab on the **Properties** interface then select **Authenticated Users**.
11. Check the **Allow** check box for the **Enroll** permission. The **Authenticated Users** group should now have **Read** and **Enroll** permissions.



12. Select the **Issuance Requirements** tab then check the box next to **This number of authorized signature**. The number entry must be set at **1**. The **Policy type required in signature** setting must

Copyright © 2008 Microsoft Corporation.
All rights reserved.

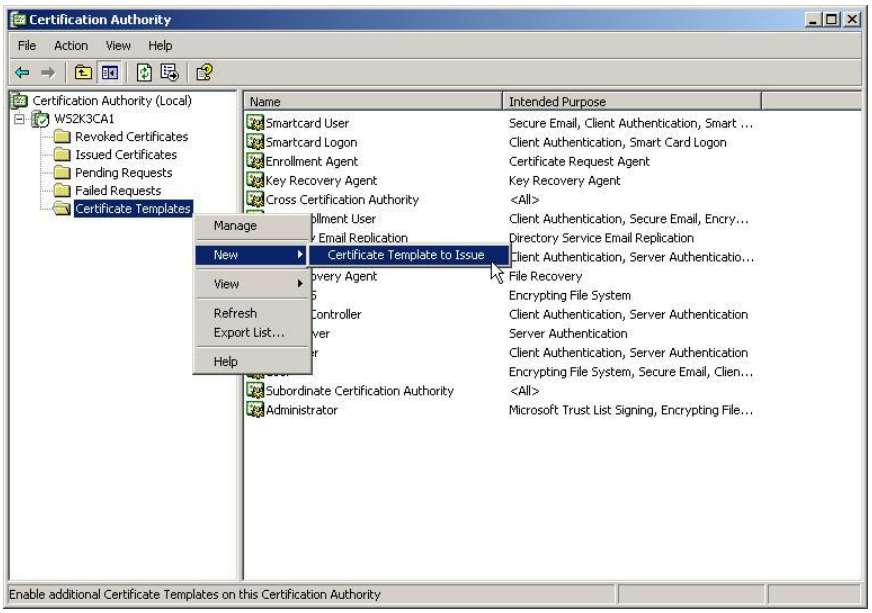
be set to **Application policy** and the **Application policy** setting must be set to **Certificate Request Agent** as shown below. Click **OK** on the **Properties** interface.



13. Repeat procedures 9 through 12 for the **Smart Card User** duplicate certificate template.

Adding smart card certificates for issuance:

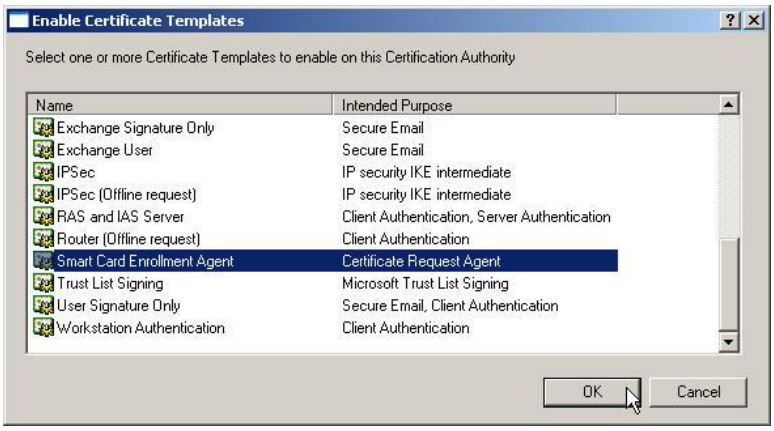
1. Log on as the CA administrator.
2. Open **Certification Authority**. Click **Start**, select **Control Panel**, double-click **Administrative Tools**, and then double-click **Certification Authority**.
3. Expand the CA node then right-click **Certificate Templates,** point to **New**, and select **Certificate Template to Issue**.



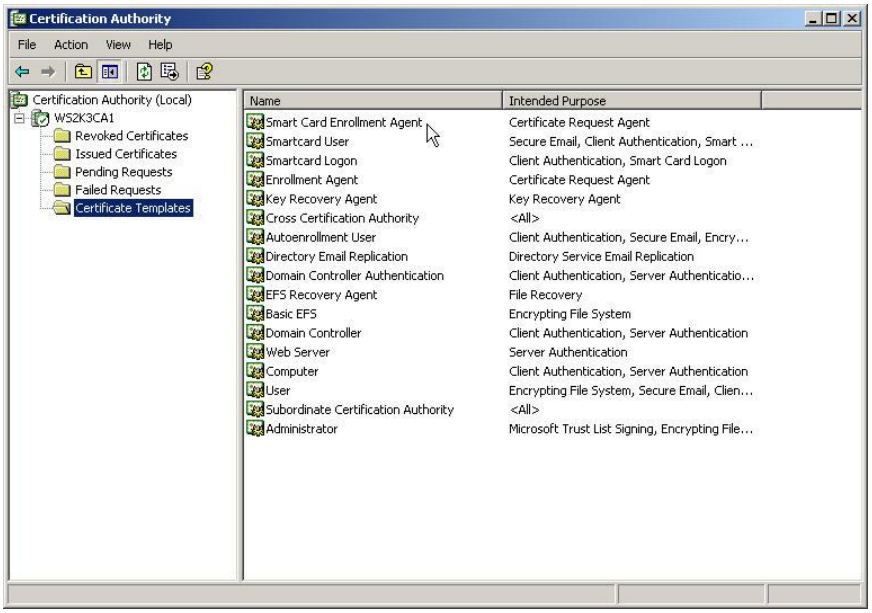
Copyright © 2008 Microsoft Corporation.

All rights reserved.

4. In the **Enable Certificate Templates** interface, select the **Smart Card Enrollment Agent** template (copy of **Enrollment Agent** template) and click **OK**.



5. The certificate template will appear in the **Certificate Templates** view of the **Certification Authority** interface and is ready to be issued.



6. Repeat the procedures above for the **Smart Card Logon** and **Smart Card User** duplicate templates.
   - If the CA will issue certificates that are only for logging on to Windows with smart cards, select the **Smart Card Logon** certificate template.
   - If the CA will issue certificates that can be used to log on to Windows with smart cards and other uses, select the **Smart Card User** certificate template.

Notes:

- The security permission setting of a certificate template indicates who is allowed to request a certificate of that type.
- The Enrollment Agent certificate does not have to be issued from the same CA that will issue certificates for smart cards, but the issuing CA for the Enrollment Agent certificate must be a trusted enterprise CA in the domain. In that case, make sure that there is an enterprise CA in the domain that is capable of issuing Enrollment Agent certificates. To do this, follow the above steps

Copyright © 2008 Microsoft Corporation.
All rights reserved.

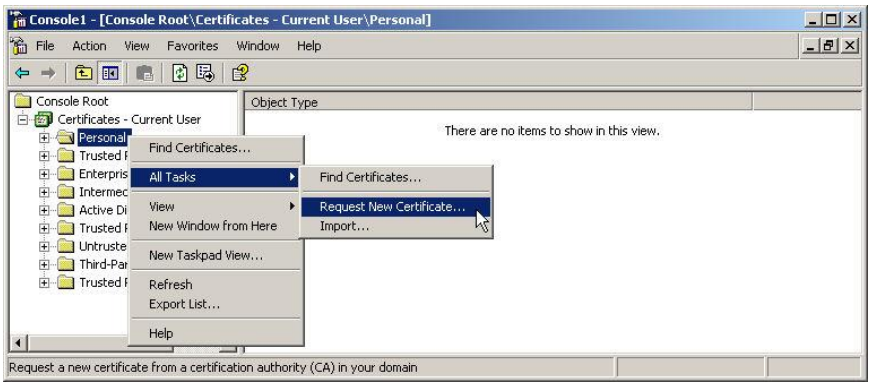
for the CA that will issue certificates that will be used for logging on to Windows with a smart card and other uses. Then follow the above steps to issue an enrollment agent certificate.

- The procedures above for management of smart card certificates only apply to Enterprise CAs.

Prepare a Smart Card Certificate Enrollment Station

To prepare a smart card certificate enrollment station the Enrollment Agent certificate must be imported to the designated Smart Card Enrollment Agent's Personal certificate store.

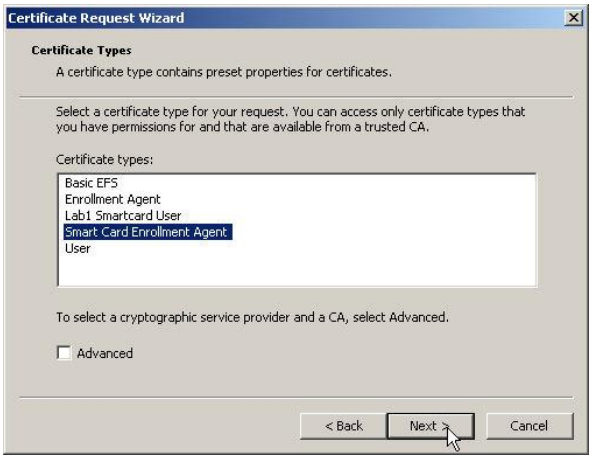
1. On the computer that will be used to enroll smart cards, install a smart card reader, following the manufacturer's instructions. See Installing a Smart Card reader.
2. Log on as the user that has been designated as the Smart Card Enrollment Agent for installing user certificates on smart cards.
3. On the taskbar, click the **Start** button, click **Run**, type **mmc**, and then click **OK**.
4. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
5. In **Snap-in**, double-click **Certificates**. If logged on as a user, the **Certificates** snap-in automatically loads. If logged on with an administrator account, select **My user account**, and then click **Finish**.
6. Click **Close** and then click **OK**.
7. Expand **Certificates - Current User**.
8. Right-click **Personal**, point to **All Tasks**, and then select **Request New Certificate**. This will initiate the **Certificate Request Wizard**.



9. Follow the **Certificate Request Wizard** instructions. At the **Certificate Types** page of the Wizard, select the **Enrollment Agent** (or **Smart Card Enrollment Agent**, if the duplicate template is created according to examples above in the "Prepare a certification authority to issue smart card certificates" subsection). Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



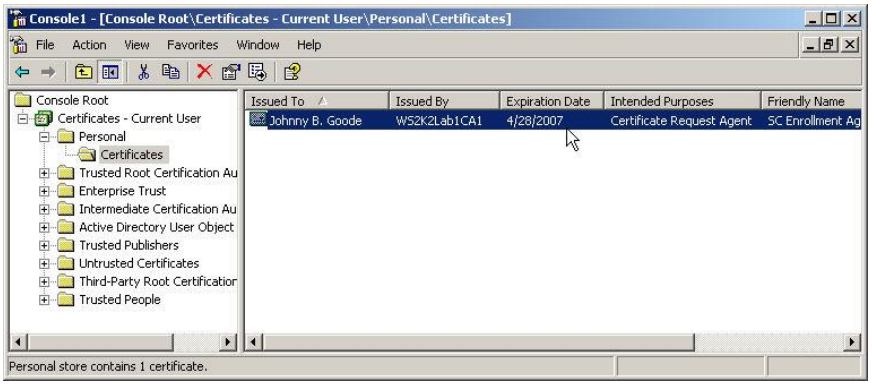
10. Type a friendly name and a description for the certificate. Click **Next**.

11. Review the settings. If corrections need to be made click the **Back** button to get to the correct page and make the appropriate corrections. If the settings are correct, click **Finish**.

12. A message will appear indicating that the request was successful. Click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

13. The enrollment agent certificate will appear in the **Certificates** store.



Notes:

- Typically the Web enrollment station (using IE as an Interface) can be used instead of the method described in this procedure. However, IE is not used in the Evaluated Configuration.
- Before requesting smart card logon certificates for users, a smart card administrator must have an Enrollment Agent certificate available to generate smart card certificate requests on the behalf of others. That is the purpose of this procedure.
- To perform this procedure, the authorized administrator must have the appropriate security permissions to administer the Enrollment Agent certificate template.
- For the Evaluated Configuration, these tasks can be performed on any computer running Windows XP Professional or a member of the Windows Server 2003 family that will be used as a smart card certificate enrollment station.

Add a Certificate to a Smart Card on Behalf of a User

To add a user certificate to a smart card on behalf of a user, the Smart Card Enrollment Agent uses the **certreq.exe** tool. **Certreq.exe** is installed with the **Windows Server 2003 Administration Tools Pack**. The Smart Card Enrollment Agent uses certreq.exe to:

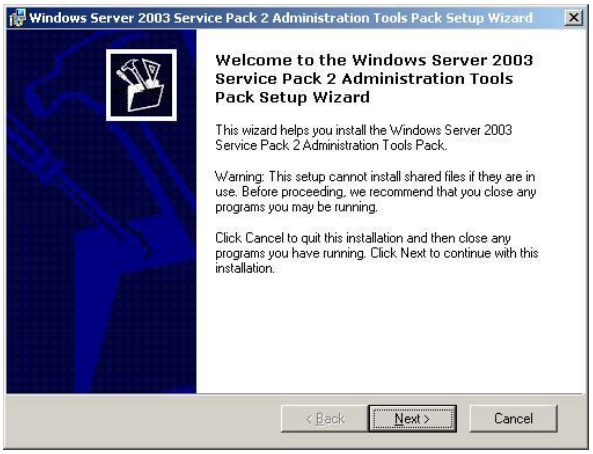
- Make the initial certificate request, using a user.inf file, that will be signed and sent to the CA;
- Sign the certificate request with the Smart Card Enrollment Agent's certificate;
- Send the sighed certificate request to the CA; and
- Accept the user certificate and place it on the smart card on behalf of the user.

To install the **Windows Server 2003 Administration Tools Pack** on a Windows Server 2003 host that has SP2 installed:

1. Log on as an authorized administrator.
2. Navigate to the **C:\WINDOWS\System32** folder and execute the **Adminpak.msi** setup program.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. Follow the Wizard to install the **Windows Server 2003 SP2 Administration Tools Pack**.



Note: Versions of the Adminpak.msi setup program must match the Service Pack installed on a server.

The procedures for using **certreq.exe** to add a user certificate to a smart card are described below. An INF file will need to be created and modified for each user. The contents of the file are shown below in Step 2.

1. Log on as the user that is designated as the Smart Card Enrollment Agent.
2. Insert the media containing the **user.inf** file or copy the file to the local hard drive. The user.inf file contains the information shown below.

```
[NewRequest]
RequestType=CMC
ProviderName=" Microsoft Base Smart Card Crypto Provider "
KeyContainer=""
KeySpec=1
ProviderType=1

[RequestAttributes]
CertificateTemplate=SmartcardLogon
RequesterName=<DomainName>\<User Name>
```

3. Edit the user.inf file by making the appropriate entries under **[RequestAttributes]**. If the **Smart Card Logon** template name has been changed for a duplicate template, enter the appropriate name for the **Certificate Template** value. For the **RequesterName** value, enter the domain and name of the user for which a certificate is being requested. For example, if the certificate request is for user *plane* (Penny Lane) in domain *WS2K3Lab1.com*, enter *WS2K3Lab1\plane* as the **RequesterName** value. If desired, save the modified user.inf file under a different name, such as *plane.inf*.
4. Open a command line interface and change directories to the location of the modified **user.inf** file.
5. Enter the following command to request a certificate on behalf of the user (in this case the user is Penny Lane – user name *plane*):

   certreq – new plane.inf plane.req

Copyright © 2008 Microsoft Corporation.
All rights reserved.

6. The **Infineon SICRYPT Smart Card Crypto Provider** interface will appear. Insert a new smart card is in the smart card reader. Click **OK**.

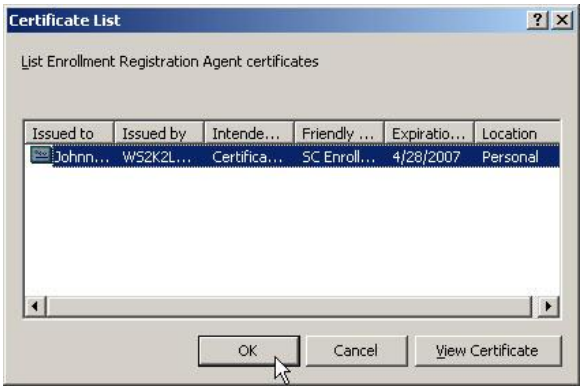
7. The **SICRYPT Smart Card-Verify Password** interface will appear. Enter the default PIN number (12345678) in the **Password** entry box and click **OK**. A request file will be created.

Note: There is an option to change the smart card PIN by selecting the **Change** button. It is a good security practice to do so, however users should be required to change their PIN to something only they know as soon as they receive the new smart card. There will be a second opportunity to change the PIN in the steps that follow.

8. At the command line interface, enter the following command to sign the certificate request file with the designated enrollment agent's certificate:

   certreq – sign plane.req plane-singned.req

9. The **Certificate List** interface will appear, select the **Smart Card Enrollment Agent** certificate and click **OK**.



10. At the command line interface, enter the following command to submit the certificate request to a CA:

    certreq – submit plane-singned.req plane.cer

11. An interface appear to allow selection of a CA. Select the CA and click **OK**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

12. Enter the following command to accept the certificate:

    certreq – accept plane.cer

13. The **SICRYPT Smart Card-Verify Password** interface will appear. Enter the default PIN number (12345678) in the **Password** entry box and click **OK.**

Note: There is an option to change the smart card PIN by selecting the **Change** button. It is a good security practice to do so, however users should be required to change their PIN to something only they know as soon as they receive the new smart card.

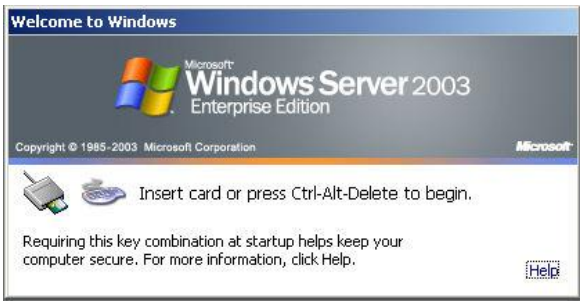
14. The certificate is placed on the smart card.

Note: After the Smart Card Enrollment Agent adds a user certificate to a smart card, the public certificate of the user may be placed into the Smart Card Enrollment Agent's **Personal** certificate store. It is recommended that the Smart Card Enrollment Agent delete those certificates from the local Personal certificates store after completing the smart card enrollment tasks.

Logging on to a Computer with a Smart Card

To log on to a computer with a Smart Card, users do not need to type **CTRL+ALT+DEL**. They simply insert the smart card into the Smart Card reader and the computer prompts them for their PIN instead of their user name and password.

1. If the computer is configured to use a smart card, the **Welcome to Windows** logon interface will show a smart card icon. Insert the smart card into the smart card reader.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. Type the PIN for the smart card when prompted by the computer. Click **OK** to log on.

Notes:

The Smart Card must be prepared by creating the appropriate credentials before using it to log on to the computer.

If the PIN entered is recognized as legitimate, this logs the user on to the computer and to the Windows Server 2003 family domain, based on the permissions assigned to the user account by the domain administrator.

If the incorrect PIN is entered for a smart card several times in a row, the user will be unable to log on to the computer using that smart card. The number of allowable invalid logon attempts before lockout occurs varies according to the smart card manufacturer. By default, the Infineon Sicrypt smart cards become locked if an incorrect PIN is entered three times in a row. A locked card can only be unlocked by an authorized administrator using the **Infineon Sicrypt Cryptographic Service Provi**der Tools (CSP Tools) and an administrator PIN.

If the smart card is inserted backwards or upside down, the Smart Card will not work. However, the user may be prompted for a PIN which will not work.

Smart Card logons only work for computers that are joined to a domain.

If a Domain Controller is not available, the Smart Card logon fails even if the user has previously logged onto the computer using the Smart Card. If the Domain Controller is available but does not have a valid CRL for the issuing CA, then the logon fails.

Changing the Smart Card PIN

All users must be required by policy to change the default smart card PIN as soon as they receive their smart card. Procedures for changing the smart card PIN are dependent on smart card vendor applications which are outside the TOE. For the Evaluated Configuration, the Sicrypt smart card from Infineon Technologies is used. To allow users the capability to change their smart card PINs the **Infineon Sicrypt Cryptographic Service Provider Tools** must be installed. The setup program for the tools can be downloaded from the Infineon Technologies Web site at http://www.infineon.com.

To install the **Infineon Sicrypt Cryptographic Service Provider Tools** on a user's computer:

1. Download the **Infineon Sicrypt Cryptographic Service Provider Tools** setup program and copy it to a transportable medium.
2. Log onto the user's workstation or server as an authorized administrator and insert the media containing the setup program.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. Execute the **Infineon Sicrypt Cryptographic Service Provider Tools** setup program and follow the Wizard to install the smart card tools.

To change a smart card PIN:

1. The smart card user logs on to the computer using a regular domain account and password (alternatively, the user may log on using the issued smart card with the default PIN).
2. Click **Start**, point to **All Programs,** point to **Infineon SICRYPT CSP Tools**, and select **SICRYPT Smart Card Admin Tool**.
3. The **SICRYPT Smart Card Admin Tool** interface will appear. Insert the smart card into the smart card reader.

4. Click the **PIN** button. Enter the current PIN number in the **PIN** entry box, then enter the new PIN in the **new PIN** box and confirm it by entering it again in the **Confirm PIN** box. Guidelines for selecting a PIN are as follow:
   - The **SICRYPT Smart Card Admin Tool** allows the PIN to be set to a minimum of four (4) characters and a maximum of eight (8). For the Evaluated Configuration, PINs must be comprised of eight (8) characters.
   - For strong security, create the PIN by using a mixture of alphabet characters, numbers, and other special characters such as #, @, or $.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

5. Click the **Change PIN** button. A message will appear indicating that the PIN of the signature card has been changed successfully. Click **OK**.
6. Close the **SICRYPT Smart Card Admin Tool** interface.

Distributed File System (DFS)

The Distributed File System (DFS) solution in the Microsoft Windows Server 2003 R2 with SP2 operating system helps administrators manage user access to data that is distributed across several servers, reduce network traffic, ensure the availability, and ensure that files on servers are backed up correctly by providing two technologies, DFS Namespaces and DFS Replication. When used together, these technologies offer simplified, fault-tolerant access to files, load sharing, and replication.

The DFS technologies provided in the R2 update of Windows Server 2003 are described below.

- **DFS Replication**. This is a new state-based, multimaster replication engine that is optimized for WAN environments. DFS Replication supports replication scheduling, bandwidth throttling, and a new byte-level compression algorithm known as remote differential compression (RDC). RDC detects insertions, removals, and re-arrangements of data in files, thereby enabling DFS Replication to replicate only the changes when files are updated. Additionally, a function of RDC called cross-file RDC can help reduce the amount of bandwidth required to replicate new files.
- **DFS Namespaces**. This technology helps administrators group shared folders located on different servers and present them to users as a virtual tree of folders known as a namespace. DFS Namespaces was formerly known as Distributed File System in Windows 2000 Server and Windows Server 2003 (prior to adding R2). A namespace provides numerous benefits, including increased availability of data, load sharing, and simplified data migration.

Key Scenarios

Although DFS Namespaces and DFS Replication are two separate technologies, when used together they provide solutions for a number of key scenarios in medium and large organizations.

- **Data collection**. The data collection scenario helps address the need to eliminate the use of recurring local backups and significantly reduce operational costs. To accomplish this, data can be replicated from several distributed servers to a server in a central location. Administrators of the centralized server can backup the data from the centrally located server, eliminating the need to

Copyright © 2008 Microsoft Corporation.

All rights reserved.

perform backups at each of the distributed servers. Centralizing backups also allows organizations to consolidate backup hardware and related management tasks.

Using RDC, DFS Replication replicates only the differences (or changes) between the servers; as a result, bandwidth used during replication is minimized.

When DFS Replication is used in conjunction with DFS Namespaces, administrators can configure a namespace so that clients of a distributed serve always connect to that server. If the distributed server becomes unavailable, its clients fail over to the central server.

- **Data distribution**. DFS Namespaces and DFS Replication can be used to publish documents, software, and line-of-business data to users throughout an organization. Although DFS Replication alone is sufficient to distribute data, using DFS Namespaces allows administrators to configure the namespace so that a folder in the namespace is hosted by multiple servers, which increases data availability and distributes the client load across servers. When browsing the namespace, users see a single folder and are not aware the folder is hosted by multiple servers. When a user opens the folder, the client computer is automatically referred to a server in its own site; if no same-site servers are available, administrators can configure the namespace to refer the client to a server that has the lowest connection cost as defined in the Active Directory.
- **File sharing**. In large organizations, users in one office often need access to shared folders and files stored at another office location or at the central data center. Although in some cases the need is collaborative, in other cases users simply need access to those files. If low latency and data availability during WAN outages is worth the tradeoff of network traffic and disk space used in the branch office, administrators can use DFS Replication to replicate files between branch servers, providing users fast access to files in their respective branch offices.

  When the shared folders are defined as folders in a namespace, users access them by browsing what appears to be a single server, giving the users a consistent place to begin browsing for files. For example, a user who travels from one office location to another will access what appears to be the same folder in the namespace, but the user is actually referred to the closest server that contains the data.

DFS Namespaces

Namespaces Size Recommendations

For stand-alone namespaces, a maximum of 50,000 folders with targets is recommended. This recommendation is based on startup times for the DFS service for large namespaces.

For domain-based namespaces, the namespace object in Active Directory should be 5 megabytes (MB) or less (equivalent to about 5,000 folders with targets). This recommendation is aimed at reducing the time and bandwidth needed to replicate the namespace object using Active Directory replication each time the namespace changes.

Note: Folders without folder targets do not count against these limits.

Security requirements for creating and managing namespaces

The following table describes the groups that can perform basic namespace tasks by default, and the method for delegating the ability to perform these tasks.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Task	Groups That Can Perform This Task By Default	Delegation Method
Create a domain-based namespace	Domain Admins group in the domain where the namespace is configured	Right-click the **Namespace** node in the console tree, and then click **Delegate Management Permissions**. The user must also be added to the Local Administrators group on the namespace server.
Add a namespace server to a domain-based namespace	Domain Admins group in the domain where the namespace is configured	Right-click the domain-based namespace in the console tree, and then click **Delegate Management Permissions**. The user must also be added to the Local Administrators group on the namespace server to be added.
Manage a domain-based namespace	Local Administrators group on each namespace server	Right-click the domain-based namespace in the console tree, and then click **Delegate Management Permissions**.
Create a stand-alone namespace	Local Administrators group on the namespace server	Add the user to the local Administrators group on the namespace server.
Manage a stand-alone namespace*	Local Administrators group on the namespace server	Right-click the stand-alone namespace in the console tree, and then click **Delegate Management Permissions**.
Create a replication group or enable DFS Replication on a folder	Domain Admins group in the domain where the namespace is configured	Right-click the **Replication** node in the console tree, and then click **Delegate Management Permissions**.

Installation Requirements

Operating system and server requirements

The following are operating system and server requirements for managing and hosting DFS within the TOE.

- Servers where namespace management tasks are performed using the DFS Management snap-in must run Windows Server 2003 R2 with SP2.
- All servers that host namespaces must run Windows Server 2003 with SP2 or Windows Server 2003 R2 with SP2.
- To support new namespace features, all domain controllers must run Windows Server 2003 with SP2 or Windows Server 2003 R2 with SP2.
- Namespaces must be created on NTFS volumes.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Client compatibility for DFS Namespaces

Within the TOE, clients that access namespaces must run one of the following operating systems:

- Windows Server 2003 R2 with SP2
- Windows Server 2003 with SP2
- Windows XP Professional with SP2

DFS Namespace installation and configuration procedures

Installing DFS on the Namespace Server

Before installing DFS on a Microsoft Windows Server 2003 with SP2 server, the operating system must first be upgraded to R2. To install R2, see procedures in the "Microsoft Windows Server 2003 R2 Requirement for ADFS and DFS Components" section of the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

1. Logon to the server designated to be the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start,** point to **Control Panel**, and then select **Add or Remove Programs**.
3. In the Add or Remove Programs interface, click **Add/Remove Windows Components**.
4. In the Windows Components Wizard, scroll down to **Distributed File System**, click **Distributed File System** to highlight it, and then click **Details**.
5. Select the **DFS Management** checkbox. Verify that the **DFS Replication Diagnostic and Configuration Tools** checkbox has been selected. This is required to be installed with DFS Management. Click **OK** and then **Next**.
6. The Configuring Components window will appear and the DFS installation will begin.
7. If prompted to insert the "Windows 2003 R2 Disc 2" CD, insert the appropriate disc into the optical drive and click **OK**. The installation will continue.
8. When prompted, click **Finish** in the Windows Components Wizard.
9. Close the Add or Remove Program interface.

Configuring DFS on the Namespace Server

1. Logon to the server designated to be the DFS Namespace server with an account that is a member of the Domain Admins group, or with an account that is a member of the local Administrators group on each server that hosts the namespace and has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click **Namespace** and select **New Namespace**. The New Namespace Wizard will appear.
4. On the Namespace Server page, enter the name of the designated namespace server or click the **Browse** button to search for the designated server name. After verifying the appropriate serve is listed in the Server text box, click **Next**.

Note: If prompted to set the DFS Service start state to Automatic and start the service, click, **Yes**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

5. On the Namespace Name and Settings page, enter the name for the new Namespace, for example, "Public". Click **Next**.
6. On the Namespace Type page, verify that **Domain-based namespace** is selected by default and click **Next**.
7. On the Review Settings and Create Namespace page, review the settings and click **Create**.
8. Click **Close** to exit the New Namespace Wizard.

Delegating management permissions for an existing namespace

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **Namespaces** node under the **DFS Management** node, right-click the namespace for which management permissions are to be delegated, and then click **Delegate Management Permissions**.
4. Type user names or group names separated by commas, click **Check Names** to verify the objects, and then click **OK**.

Sharing a Folder on the DFS Namespace Server

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group, or with an account that is a member of the local Administrators group on each server that hosts the namespace and has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **Namespaces** node under the **DFS Management** node, right-click the namespace, or a folder within a namespace, to share the folder under and select **New Folder**.
4. On the **New Folder** dialog box, enter the display name for the DFS shared folder in the **Name** text box.
5. Click **Add** to begin adding the folder targets.
6. In the **Add Folder Target** dialog box, enter the Universal Naming Convention (UNC) path to the folder target, for example, \\ServerName\SharedFolder\Folder. If the UNC path is not known follow the method below:
   - Click **Browse** to browse the network to locate the share.
   - In the **Browse for Shared Folders** dialog box, enter the server name directly in the **Server** text box or click **Browse** to locate the server.
   - The **Select Computer** window will appear. Type the name of the server, or enough of the server name to uniquely identify the server, where the share is located then click **Check Names** then click **OK**.
   - Click **Show Shared Folders**. The shared folders that reside on the chosen server will now appear in the Browse for Shared Folders window. Click on the desired share to highlight it then click the **OK** button.
   - Verify the UNC path of the share in the Add Folder Target window and click **OK**.
7. Click **OK**.
8. The DFS shared folder just created will now appear under the namespace.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Browsing to a DFS share from a Client Machine

1. Logon using a domain user account to a client machine that is a member of the same domain as the DFS server.
2. Click **Start**, and then select **My Computer**.
3. In the **Other Places** section of the **System Tasks** pane on the left hand side of the **My Computer** window, click on **My Network Places**.
4. In the **Other Places** section of the **Network Tasks** pane on the left hand side of the **My Computer** window, click on **Entire Network**.
5. Double-click on the **Microsoft Windows Network** icon.
6. Double-click the domain icon for the domain where the DFS Namespace server is located.
7. Double click the server icon for the DFS Namespace server. The shared folder(s) will be displayed.
8. Double-click the desired shared folder to access it.

DFS Replication

DFS Replication Requirements

The following sections describe the various requirements of DFS Replication that apply to all scenarios described in this guide.

Active Directory requirements for DFS Replication

- Active Directory must be deployed in the organization.
- The Active Directory schema must be updated to include the new DFS Replication classes and attributes. These schema changes are provided on the second Windows Server 2003 R2 operating system CD. Therefore, within the TOE, domain controllers must be running Windows Server 2003 R2 with SP2 (can include Standard, Enterprise, or Datacenter editions).
- All members of a replication group must be in the same forest. Replication cannot be enabled for servers across different forests.

Operating system requirements for using and managing DFS Replication

Within the TOE, the servers that will participate in DFS Replication must run Windows Server 2003 R2 with SP2. After installing Windows Server 2003 R2, the DFS Replication Service must be installed on each server that will take part in replication, and the DFS Management snap-in must be installed on one server to manage replication. Replicated folders must be stored on NTFS volumes.

Security requirements for creating and managing DFS Replication

The following table describes the groups that can perform basic DFS Replication tasks by default, and the method for delegating the ability to perform these tasks.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Task	Users or Groups That Can Perform This Task By Default	Delegation Method
Create a replication group or enable DFS Replication on a folder that has folder targets	Domain Admins group in the domain where the replication group will be created.	Right-click the **Replication** node in the console tree, and then click **Delegate Management Permissions**.
Administer a replication group	Domain Admins group in the domain where the replication group is configured, or the creator of the replication group.	Right-click the replication group in the console tree, and then click **Delegate Management Permissions**.
Add a server to a replication group	If the server is a member server, the user must be a member of the local Administrators group of the server to add. If the server is a domain controller, the user must be a member of the Domain Admins group in the domain where the server is located.	Add the user to local Administrators group of the member server to add, or add the user to the Domain Admins group of the domain controller to add.

When delegating the ability to create and administer replication groups, note the following two important considerations:

- If a user or group is delegated the ability to create replication groups, and the user or group are later removed from the delegation list, there is no change to the security settings on existing replication groups.
- If a user or group is delegated the ability to administer a specific replication group, and the user or group are later removed from the delegation list, there is no change to the security settings on any existing configuration data. For example, if the user who is being removed had created a connection in the replication group, then the user would still have permissions to edit that connection because the user is the owner of the Active Directory object that contains the configuration information for the connection. If this is the case, as a domain administrator, edit the ownership of the Active Directory object to change it to another authorized user.

DFS Replication installation and configuration procedures

Installing DFS Replication

If DFS Replication is going to be used, the Active Directory schema must first be updated to install the Active Directory components of DFS Replication. To upgrade the schema, on the schema operations master, run adprep.exe /forestprep. The adprep.exe command-line tool is available in the Cmpnents\R2\Adprep folder on the second Windows Server 2003 R2 installation CD.

Note: The DFS Replication Service must also be installed on each file server that will be part of the replication group. Follow the procedure to install the DFS replication service on each file server.

1. Logon to the server designated to be the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start,** point to **Control Panel**, and then select **Add or Remove Programs**.
3. In the Add or Remove Programs interface, click **Add/Remove Windows Components**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

4. In the Windows Components Wizard, scroll down to **Distributed File System**, click **Distributed File System** to highlight it, and then click **Details**.
5. Select the **DFS Replication Service** checkbox. Verify that the **DFS Replication Diagnostic and Configuration Tools** checkbox has been selected. This is required to be installed with DFS Replication Service. Click **OK** and then **Next**.
6. The Configuring Components window will appear and the DFS installation will begin.
7. If prompted to insert the "Windows 2003 R2 Disc 2" CD, insert the appropriate disc into the optical drive and click **OK**. The installation will continue.
8. When prompted, click **Finish** in the Windows Components Wizard window.
9. Close the Add or Remove Program interface.

Creating a Multi-Purpose Replication Group with Mesh Topology

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click **Replication**, then select **New Replication Group**. The **New Replication Group Wizard** starts.
4. On the Replication Group Type page select **Multi-purpose replication group** then click **Next**.
5. On the Name and Domain page, type in the desired replication group name for the **Name of replication group**. Enter a description of this replication group, if desired, under **Optional description of replication group**.
6. Verify the correct domain has been selected under **Domain**. If not, click **Browse** and select the correct domain from the Browse for Domain dialog, then click **OK**.
7. Click **Next**.
8. In the Replication Group Members page, click the **Add** button.
9. In the **Select Computers** dialog, type in the computer names of the desired file servers separated by semicolons to add to the replication group, then click **Check Names**. Click **OK** when finished.
10. Click **Next**.
11. On the Topology Selection page, verify that **Full mesh** is selected and click **Next**.
12. On the Replication Group Schedule and Bandwidth page, configure the replication schedule and specify the bandwidth for DFS Replication.
    - For continuous replication, select **Replicate continuously using the specified bandwidth**. Using the **Bandwidth** dropdown menu, select the maximum amount of bandwidth that the DFS Replication service should use.
    - To configure a replication schedule, select **Replicate during the specified times**. Click **Edit Schedule**. In the Edit Schedule dialog, highlight each period of time and specify the maximum bandwidth for DFS replication to use during that period. Repeat the previous step for each designated period of replication. When complete, click **OK**.
13. Click **Next**.
14. On the Primary Member page, use the **Primary member** dropdown menu to select the server that contains the content to be replicated to other members, then click **Next**.
15. On the Folders to Replicate page, click **Add**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

16. On the Add Folder to Replicate dialog:
    - Type the path of the folder that should be replicated in the **Local path of folder to replicate** or click **Browse** and then navigate to the folder on the primary member that will be replicated to the other replication group members.
    - Determine the method to set the replicated folder name
    - Select **Use name based on path** to use the existing name.
    - Select Use custom name to enter a replicated folder name that is not the actual folder name.
    - To set the NTFS permissions on the replicated folder, click **Permissions**. Select Existing permissions if the current NTFS permissions are adequate. Select **Custom permissions** and then click **Edit permissions** to establish the NTFS permissions on the replicated folder. Establish the desired NTFS permissions using standard procedures in the **Permissions for Folder** dialog, Click **OK** when finished.
    - Click **OK**. If the path entered does not exist on the primary member, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the Add Folder to Replicate dialog and change the local path of the folder to replicate.
    - Repeat the steps above as necessary to add all folders to replicate into the Replication Group.
17. Click **Next** to continue.
18. On the Local Path of *[replicated folder name]* on Other Members page, for each member of the Replication Group, click on the Member in the **Member details** section and then click **Edit**. In the Edit Local Path dialog:
    - Select **Disabled** to prevent the replication of the replicated folder to that member of the replication group, or
    - Select **Enabled** to enter the local path where the replicated folder will be stored on the other member(s) of the replication group. In **Local path of folder**, type the path of the folder on the member where the replicated folder should be stored or click **Browse** and then navigate to the folder on the member that will be used for replication of the replicated folder. To create a folder on the replication partner, highlight the desired parent folder, then click the **Make New Folder** button. Type a name for the newly created folder then click **OK** to continue. If the path entered does not exist on the other replication group members, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the previous dialog and change the local path of the replicated folder. Click **OK**.
19. Click **Next**.
20. If there are multiple replicated folders, the next Local Path of *[shared folder name]* on Other Members page will appear. Repeat the previous step for each folder. Click **Next**.
21. On the Review Settings and Create Replication Group page, click **Create**.
22. On the Confirmation page, if all tasks complete with a **Success** status, click close. If the status of any task is **Error**, click the **Errors** tab to troubleshoot the errors. When all errors have been resolved, click **Close**.
23. A **Replication Delay** dialog will appear notifying that there may be a delay in replication depending on Active Directory replication latency as well as the polling interval. Click **OK** after reviewing the message.
24. The Replication Group just created will appear under **Replication** in the DFS Management interface.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Creating a Multi-Purpose Replication Group with Hub and Spoke Topology

For the hub and spoke topology, there must be at least three members of the replication group.

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click **Replication**, then select **New Replication Group**. The **New Replication Group Wizard** starts.
4. On the Replication Group Type page select **Multi-purpose replication group** the click **Next**.
5. On the Name and Domain page, type in the desired replication group name for the **Name of replication group**. Enter a description of this replication group, if desired, under **Optional description of replication group**.
6. Verify the correct domain has been selected under **Domain**. If not, click **Browse** and select the correct domain from the Browse for Domain dialog, then click **OK**.
7. Click **Next**.
8. In the Replication Group Members page, click the **Add** button.
9. In the **Select Computers** dialog, type in the computer names of the desired file servers separated by semicolons to add to the replication group, then click **Check Names**. Click **OK** when finished.
10. Click **Next**.
11. On the Topology Selection page, verify that **Hub and spoke** is selected and click **Next**.
12. On the Hub Members page, in the **Spoke members** column, click on each replication group member that will be a Hub member, then click **Add**. Control-click on multiple members to add them as a group to the **Hub members** column. At least one member must be added to the Hub members column to continue. Click **Next**.
13. On the Hub and Spoke Connections page, review the Connections. If no modifications are required, click **Next**. If modifications to the connections are required, click on the connection to be modified and click **Edit**. Change details of the connection as desired, then click **OK** and then click **Next**.
14. On the Replication Group Schedule and Bandwidth page, configure the replication schedule and specify the bandwidth for DFS Replication.
    - For continuous replication, select **Replicate continuously using the specified bandwidth**. Using the **Bandwidth** dropdown menu, select the maximum amount of bandwidth that the DFS Replication service should use.
    - To configure a replication schedule, select **Replicate during the specified times**. Click **Edit Schedule**. In the Edit Schedule dialog, highlight each period of time and specify the maximum bandwidth for DFS replication to use during that period. Repeat the previous step for each designated period of replication. When complete, click **OK**.
15. Click **Next**.
16. On the Primary Member page, use the **Primary member** dropdown menu to select the server that contains the content to be replicated to other members, and then click **Next**.
17. On the Folders to Replicate page, click **Add**.
18. On the Add Folder to Replicate dialog:
    - Type the path of the folder that should be replicated in the **Local path of folder to replicate** or click **Browse** and then navigate to the folder on the primary member that will be replicated to the other replication group members.
    - Determine the method to set the replicated folder name.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Select **Use name based on path** to use the existing name.
- Select Use custom name to enter a replicated folder name that is not the actual folder name.
- To set the NTFS permissions on the replicated folder, click **Permissions**. Select Existing permissions if the current NTFS permissions are adequate. Select **Custom permissions** and then click **Edit permissions** to establish the NTFS permissions on the replicated folder. Establish the desired NTFS permissions using standard procedures in the **Permissions for Folder** dialog, Click **OK** when finished.
- Click **OK**. If the path entered does not exist on the primary member, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the Add Folder to Replicate dialog and change the local path of the folder to replicate.
- Repeat the steps above as necessary to add all folders to replicate into the Replication Group.

19. Click **Next**.
20. On the Local Path of *[replicated folder name]* on Other Members page, for each member of the Replication Group, click on the Member in the **Member details** section and then click **Edit**. In the Edit Local Path dialog:
    - Select **Disabled** to prevent the replication of the replicated folder to that member of the replication group.
    - Select **Enabled** to enter the local path where the replicated folder will be stored on the other member(s) of the replication group. In **Local path of folder**, type the path of the folder on the member where the replicated folder should be stored or click **Browse** and then navigate to the folder on the member that will be used for replication of the replicated folder. To create a folder on the replication partner, highlight the desired parent folder, then click the **Make New Folder** button. Type a name for the newly created folder then click **OK** to continue. If the path entered does not exist on the other replication group members, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the previous dialog and change the local path of the replicated folder. Click **OK**.
21. Click **Next**.
22. If there are multiple replicated folders, the next Local Path of *[shared folder name]* on Other Members page will appear. Repeat the previous step for each folder. Click **Next**.
23. On the Review Settings and Create Replication Group page, click **Create**.
24. On the Confirmation page, if all tasks complete with a **Success** status, click close. If the status of any task is **Error**, click the **Errors** tab to troubleshoot the errors. When all errors have been resolved, click **Close**.
25. A **Replication Delay** dialog will appear notifying that there may be a delay in replication depending on Active Directory replication latency as well as the polling interval. Click **OK** after reviewing the message.
26. The Replication Group just created will appear under **Replication** in the DFS Management console.

Creating a Multi-Purpose Replication Group with no Topology

For the hub and spoke topology, there must be at least three members of the replication group.

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click **Replication**, then select **New Replication Group**. The **New Replication Group Wizard** starts.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

4. On the Replication Group Type page select **Multi-purpose replication group** the click **Next**.
5. On the Name and Domain page, type in the desired replication group name for the **Name of replication group**. Enter a description of this replication group, if desired, under **Optional description of replication group**.
6. Verify the correct domain has been selected under **Domain**. If not, click **Browse** and select the correct domain from the Browse for Domain dialog, then click **OK**.
7. Click **Next**.
8. In the Replication Group Members page, click the **Add** button.
9. In the **Select Computers** dialog, type in the computer names of the desired file servers separated by semicolons to add to the replication group, then click **Check Names**. Click **OK** when finished.
10. Click **Next**.
11. On the Topology Selection page, verify that **No topology** is selected and click **Next**.
12. A warning will appear notifying that no replication will take place until a custom topology is created after the current wizard is completed. Click **OK** after reviewing the message.
13. On the Primary Member page, use the **Primary member** dropdown menu to select the server that contains the content to be replicated to other members, and then click **Next**.
14. On the Folders to Replicate page, click **Add**.
15. On the Add Folder to Replicate dialog:
    - Type the path of the folder that should be replicated in the **Local path of folder to replicate** or click **Browse** and then navigate to the folder on the primary member that will be replicated to the other replication group members.
    - Determine the method to set the replicated folder name.
    - Select **Use name based on path** to use the existing name.
    - Select Use custom name to enter a replicated folder name that is not the actual folder name.
    - To set the NTFS permissions on the replicated folder, click **Permissions**. Select Existing permissions if the current NTFS permissions are adequate. Select **Custom permissions** and then click **Edit permissions** to establish the NTFS permissions on the replicated folder. Establish the desired NTFS permissions using standard procedures in the **Permissions for Folder** dialog, Click **OK** when finished.
    - Click **OK**. If the path entered does not exist on the primary member, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the Add Folder to Replicate dialog and change the local path of the folder to replicate.
    - Repeat the steps above as necessary to add all folders to replicate into the Replication Group.
16. Click **Next**.
17. On the Local Path of *[replicated folder name]* on Other Members page, for each member of the Replication Group, click on the Member in the **Member details** section and then click **Edit**. In the Edit Local Path dialog:
    - Select **Disabled** to prevent the replication of the replicated folder to that member of the replication group.
    - Select **Enabled** to enter the local path where the replicated folder will be stored on the other member(s) of the replication group. In **Local path of folder**, type the path of the folder on the member where the replicated folder should be stored or click **Browse** and then navigate to the folder on the member that will be used for replication of the replicated folder. To create a folder

Copyright © 2008 Microsoft Corporation.

All rights reserved.

on the replication partner, highlight the desired parent folder, then click the **Make New Folder** button. Type a name for the newly created folder then click **OK** to continue. If the path entered does not exist on the other replication group members, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the previous dialog and change the local path of the replicated folder. Click **OK**.

18. Click **Next**.
19. If there are multiple replicated folders, the next Local Path of *[shared folder name]* on Other Members page will appear. Repeat the previous step for each folder. Click **Next**.
20. On the Review Settings and Create Replication Group page, click **Create**.
21. On the Confirmation page, if all tasks complete with a **Success** status, click close. If the status of any task is **Error**, click the **Errors** tab to troubleshoot the errors. When all errors have been resolved, click **Close**.
22. A **Replication Delay** dialog will appear notifying that there may be a delay in replication depending on Active Directory replication latency as well as the polling interval. Click **OK** after reviewing the message.
23. The Replication Group just created will appear under **Replication** in the DFS Management console.

Create a topology

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click the replication group to create a new topology for, then select **New Topology**. The **New Topology Wizard** starts.
4. On the Topology Selection page, select the type of topology to create.
   - For a hub and spoke topology, verify that **Hub and spoke** is selected and click **Next**. On the Hub Members page, in the **Spoke members** column, click on each replication group member that will be a Hub member, then click **Add**. Control-click on multiple members to add them as a group to the **Hub members** column. At least one member must be added to the Hub members column to continue. Click **Next**. On the Hub and Spoke Connections page, review the Connections. If no modifications are required, click **Next**. If modifications to the connections are required, click on the connection to be modified and click **Edit**. Change details of the connection as desired, then click **OK** and then click **Next**.
   - For a mesh topology, verify that **Mesh** is selected and click **Next**.
5. On the Replication Group Schedule and Bandwidth page, configure the replication schedule and specify the bandwidth for DFS Replication.
   - For continuous replication, select **Replicate continuously using the specified bandwidth**. Using the **Bandwidth** dropdown menu, select the maximum amount of bandwidth that the DFS Replication service should use.
   - To configure a replication schedule, select **Replicate during the specified times**. Click **Edit Schedule**. In the Edit Schedule dialog, highlight each period of time and specify the maximum bandwidth for DFS replication to use during that period. Repeat the previous step for each designated period of replication. When complete, click **OK**.
6. Click **Next**.
7. On the Review Settings and Create Replication Group page, click **Create**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

8. On the Confirmation page, if all tasks complete with a **Success** status, click close. If the status of any task is **Error**, click the **Errors** tab to troubleshoot the errors. When all errors have been resolved, click **Close**.
9. A **Replication Delay** dialog may appear notifying that there may be a delay in replication depending on Active Directory replication latency as well as the polling interval. Click **OK** after reviewing the message.

Creating a replicated folder

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click the replication group to create a new replicated folder for, then select **New Replicated Folder**s. The **New Replicated Folder**s **Wizard** starts.
4. On the Primary Member page, use the **Primary member** dropdown menu to select the server that contains the content to be replicated to other members, then click **Next**.
5. On the Folders to Replicate page, click **Add**.
6. On the Add Folder to Replicate dialog:
   - Type the path of the folder that should be replicated in the **Local path of folder to replicate** or click **Browse** and then navigate to the folder on the primary member that will be replicated to the other replication group members.
   - Determine the method to set the replicated folder name
   - Select **Use name based on path** to use the existing name.
   - Select Use custom name to enter a replicated folder name that is not the actual folder name.
   - To set the NTFS permissions on the replicated folder, click **Permissions**. Select Existing permissions if the current NTFS permissions are adequate. Select **Custom permissions** and then click **Edit permissions** to establish the NTFS permissions on the replicated folder. Establish the desired NTFS permissions using standard procedures in the **Permissions for Folder** dialog, Click **OK** when finished.
   - Click **OK**. If the path entered does not exist on the primary member, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the Add Folder to Replicate dialog and change the local path of the folder to replicate.
   - Repeat the steps above as necessary to add all folders to replicate into the Replication Group.
7. Click **Next**.
8. On the Local Path of *[replicated folder name]* on Other Members page, for each member of the Replication Group, click on the Member in the **Member details** section and then click **Edit**. In the Edit Local Path dialog:
   - Select **Disabled** to prevent the replication of the replicated folder to that member of the replication group.
   - Select **Enabled** to enter the local path where the replicated folder will be stored on the other member(s) of the replication group. In **Local path of folder**, type the path of the folder on the member where the replicated folder should be stored, or click **Browse** and then navigate to the folder on the member that will be used for replication of the replicated folder. To create a folder on the replication partner, highlight the desired parent folder, then click the **Make New Folder** button. Type a name for the newly created folder then click **OK** to continue. If the path entered

Copyright © 2008 Microsoft Corporation.

All rights reserved.

does not exist on the other replication group members, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the previous dialog and change the local path of the replicated folder. Click **OK**.

9. Click **Next**.
10. If there are multiple replicated folders, the next Local Path of *[shared folder name]* on Other Members page will appear. Repeat the previous step for each folder. Click **Next**.
11. On the Review Settings and Create Replication Group page, click **Create**.
12. On the Confirmation page, if all tasks complete with a **Success** status, click close. If the status of any task is **Error**, click the **Errors** tab to troubleshoot the errors. When all errors have been resolved, click **Close**.
13. A **Replication Delay** dialog will appear notifying that there may be a delay in replication depending on Active Directory replication latency as well as the polling interval. Click **OK** after reviewing the message.

Adding a member to a replication group

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click the replication group to create a new replicated folder for, then select **New Member**. The **New Member Wizard** starts.
4. On the New Members page, in the type in the computer name of the new member server to add to the replication group or click **Browse**. In the **Select Computers** dialog, type in the computer name of the new member server, then click **Check Names**. Click **OK** when finished.
5. Click **Next**.
6. On the Local Path of Replicated Folders page, for each replicated folder in the Replication Group, click on the **Name** in the **Replicated folders** section and then click **Edit**. In the Edit Local Path dialog:
   - Select **Disabled** to prevent the replication of the replicated folder to that member of the replication group.
   - Select **Enabled** to enter the local path where the replicated folder will be stored on the other member(s) of the replication group. In **Local path of folder**, type the path of the folder on the member where the replicated folder should be stored, or click **Browse** and then navigate to the folder on the member that will be used for replication of the replicated folder. To create a folder on the replication partner, highlight the desired parent folder, then click the **Make New Folder** button. Type a name for the newly created folder then click **OK** to continue. If the path entered does not exist on the other replication group members, a **Create Path** dialog will open and ask if the path should be created. Click **Yes** to have the path created or click **No** to return to the previous dialog and change the local path of the replicated folder. Click **OK**.
7. Click **Next**.
8. On the Connections page, click on each the members in the **Available members** column that will replicate with the new member and then click Add. Control-click on multiple members to add them as a group to the **Members that will replicate with new member** column. At least one member must be added to the **Members that will replicate with new member** column to continue.
9. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

10. On the replication schedule page, configure the replication schedule and specify the bandwidth for DFS Replication:
    - Select **Replicate group schedule** to use the existing group replication schedule and bandwidth settings. Click **View Schedule** to review the existing schedule.
    - Select **Custom connection schedule** to create a custom schedule. Click **Edit Schedule**. In the Edit Schedule dialog, highlight each period of time and specify the maximum bandwidth for DFS replication to use during that period. Repeat the previous step for each designated period of replication. When complete, click **OK**.
11. Click **Next**.
12. On the Review Settings and Create Replication Group page, click **Create**.
13. On the Confirmation page, if all tasks complete with a **Success** status, click close. If the status of any task is **Error**, click the **Errors** tab to troubleshoot the errors. When all errors have been resolved, click **Close**.
14. A **Replication Delay** dialog will appear notifying that there may be a delay in replication depending on Active Directory replication latency as well as the polling interval. Click **OK** after reviewing the message.

Removing a member from a replication group

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **Replication** node under the **DFS Management** node, click the replication group that the member will be deleted from, then select the **Member** tab in the center pane.
4. Right-click on the member that will be deleted, select **Delete Member**.
5. If the member contains a replicated folder that is a folder target in a namespace, a confirmation dialog will open. In the Confirm Delete Member dialog, select **Delete the member and remove the member as a target in the namespace** to stop replication of the replicated folder, remove the member form the replication group, and remove the member as a target in the namespace. Select **Delete the member only** to stop replication of the replicated folder and remove the member form the replication group, but leave the member as a target in the namespace.
6. Click **OK** when finished.
7. A **Delete Member** dialog will appear notifying that the member might continue to replicate due to Active Directory replication latency. Click **OK** after reviewing the message.

Creating a connection

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **DFS Management** node, right-click the replication group to create a new connection in, then select **New Connection**.
4. In the New connection dialog, configure the details of the new connection:
    - Using the pull-down menus in the **Sending member** section, enter the details for the sending member.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Using the pull-down menus in the **Receiving member** section, enter the details for the sending member.
- In the **Select the schedule for this connection** section, configure the replication schedule and specify the bandwidth for DFS Replication. Select **Replicate group schedule** to use the existing group replication schedule and bandwidth settings. Click **View Schedule** to review the existing schedule. To create a custom schedule, select **Custom connection schedule**. Click **Edit Schedule**. In the Edit Schedule dialog, highlight each period of time and specify the maximum bandwidth for DFS replication to use during that period. Repeat the previous step for each designated period of replication.
- To create a second connection for two-way replication between the sending and receiving members, select **Create a second connection in the opposite direction**.

5. Click **OK** after reviewing the message.

Removing a connection from a replication group

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **Replication** node under the **DFS Management** node, click the replication group that the member will be deleted from, then select the **Connections** tab in the center pane.
4. Right-click on the member that will be deleted, select **Delete**.
5. A Confirm **Delete Connection** dialog will appear. Click **Yes** after reviewing the message.

Delegating the ability to create replication groups

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
3. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
4. In the console tree, right-click the **Replication** node, and then click **Delegate Management Permissions**.
5. To add a user or group to the delegation list, click **Add**.

Delegating the ability to manage an existing replication group

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **Replication** node, right-click the replication group, and then click **Delegate Management Permissions**.
4. Type the name of the user or group to which management permissions are to be delegated, and then click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Creating a diagnostic report for DFS Replication

1. Logon to the DFS Namespace server with an account that is a member of the Domain Admins group.
2. Click **Start**, point to **Administrative Tools**, and then select **DFS Management**.
3. In the console tree, under the **Replication** node, right-click the replication group for which a diagnostic report is to be created, and then click **Create Diagnostic Report**.
4. Follow the instructions in the **Diagnostic Report Wizard**.

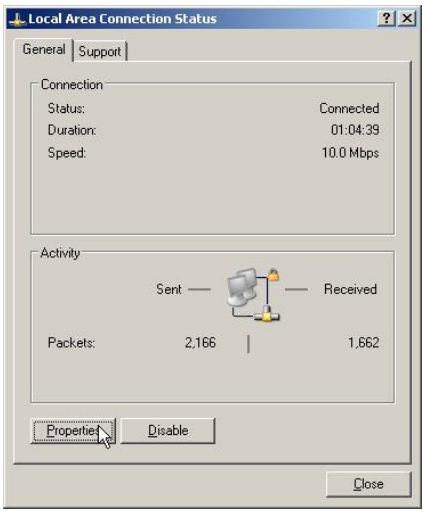
Notes: The amount of time necessary to generate a diagnostic report will vary based on a number of factors, including: DFS Replication health; the number of replicated folders; available server resources (for example, CPU, memory, and so forth); WAN availability (connectivity, bandwidth, and latency); and the chosen reporting options (backlog and file system enumeration). Because of the potential delay in creating diagnostic reports, we recommend creating diagnostic reports for no more than 50 servers at a time.

Routine Operations

Setting IP Address Information and Host Security

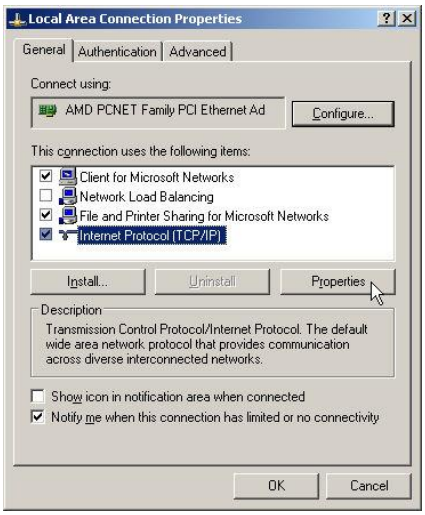
Use the following procedure to configure the IP address and required networking information for a computer, as well as IP security and network traffic filtering:

1. Log on as an authorized administrator.
2. Click **Start**, point to **Control Panel**, point to **Network Connections**, and select **Local Area Connection**.
3. On the **General** tab of the **Local Area Connection Status** interface, click the **Properties** button.

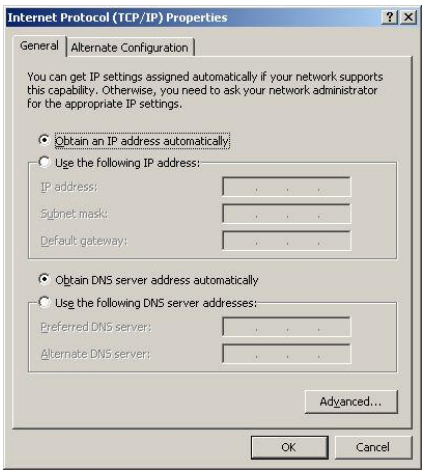


4. The **Local Area Connection Properties** window will appear. Select **Internet Protocol (TCP/IP)** and click the **Properties** button.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



5. The **Internet Protocol (TCP/IP) Properties** interface will appear. From this window, an authorized administrator can either assign a static IP address or set the computer to automatically obtain the IP address through a DHCP service.

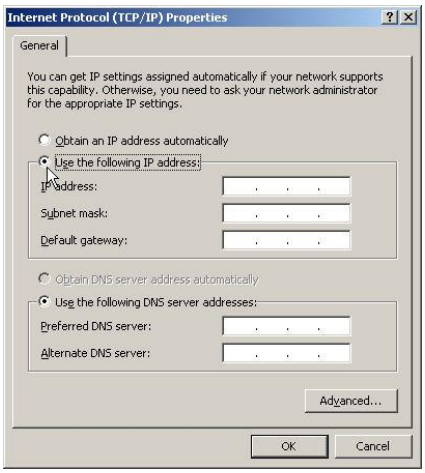


6. If the **Obtain an IP address automatically** radio button is selected, the authorized administrator can then choose to either obtain all other network information automatically by selecting the **Obtain DNS server address automatically** radio button, or set the information by selecting the **Use the following DNS sever address:** radio button.

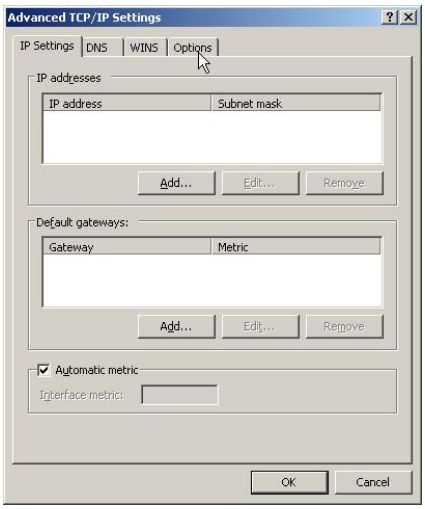
7. If the **Use the following IP address:** radio button is selected, the authorized administrator can then enter static IP address information for the computer, including subnet mask, default gateway, and DNS information.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

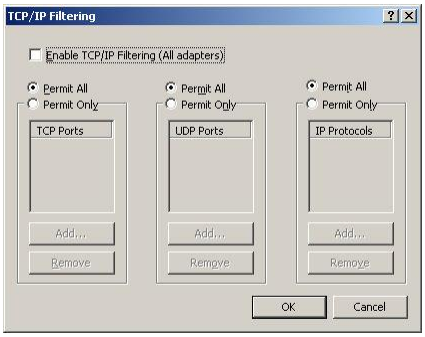


8. Selecting the **Advanced…** button opens the **Advanced TCP/IP Settings** window, which allows the authorized administrator to set additional network information such as default gateways, DNS, WINS, and optional settings for IP security and TCP/IP filtering.



9. To enable IP filtering, select the **Options** tab. Within the Options tab view window, highlight the **TCP/IP** entry under **Optional settings:** and click on the **Properties** button. The **IP Security** window will appear. Enable IP filtering by checking the **Enable TCP/IP Filtering (All adapters)** check box.

10. The default is to permit all traffic. To deny all traffic and define specific port traffic that will be allowed, select the **Permit Only** radio buttons for **TCP Ports**, **UDP Ports**, or **IP Protocols** and select the respective **Add…** buttons to specify the port traffic that is to be allowed access for the computer.



Copyright © 2008 Microsoft Corporation.

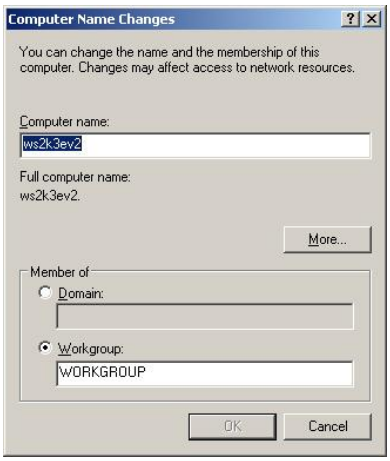
All rights reserved.

Joining a Computer to a Domain or Workgroup

Use the following procedure to join a Windows Server 2003 computer to a Windows Server 2003 network Domain:

1. Make sure the computer is configured with the appropriate network information, including the address of the local DNS server.
2. Click **Start**, right-click on **My Computer** and select **Properties**. **System Properties** window will appear. Select the **Computer Name** tab.

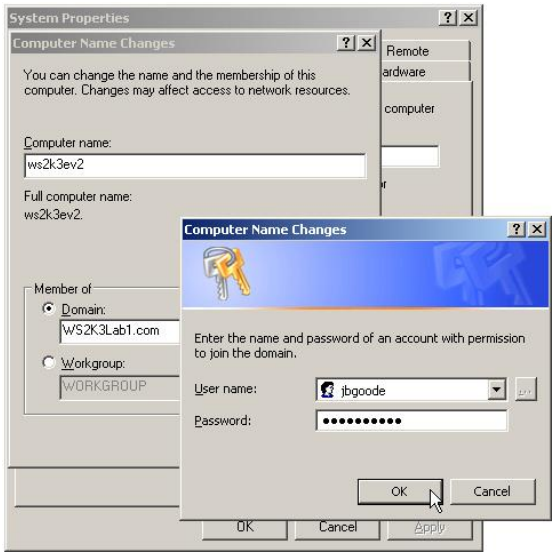
3. Click the **Change** button. The **Computer Name Changes** interface will appear.



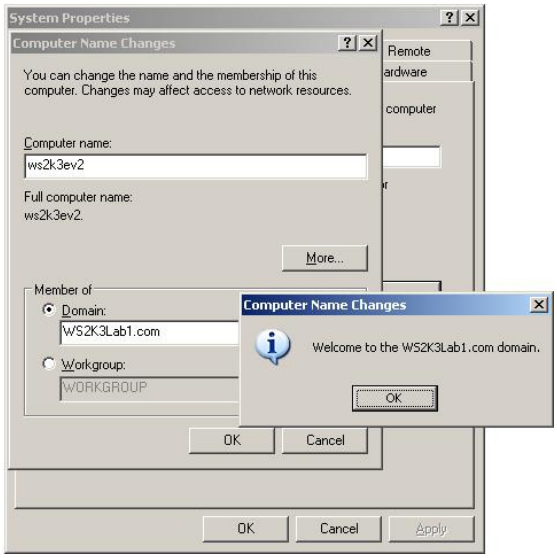
4. For this example, select the **Domain** radio button and enter the name of the desired Windows Server 2003 domain in the corresponding text box. Click the **OK** button.
5. At the password prompt, enter the name and password of an authorized administrator account that has permissions to join computers to the domain and click the **OK** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



6. Once the computer is successfully accepted into the Domain, a welcome message will appear on the screen.



7. Click the **OK** button on all windows and reboot the computer to allow the changes to take effect.

Remove a Computer from a Domain

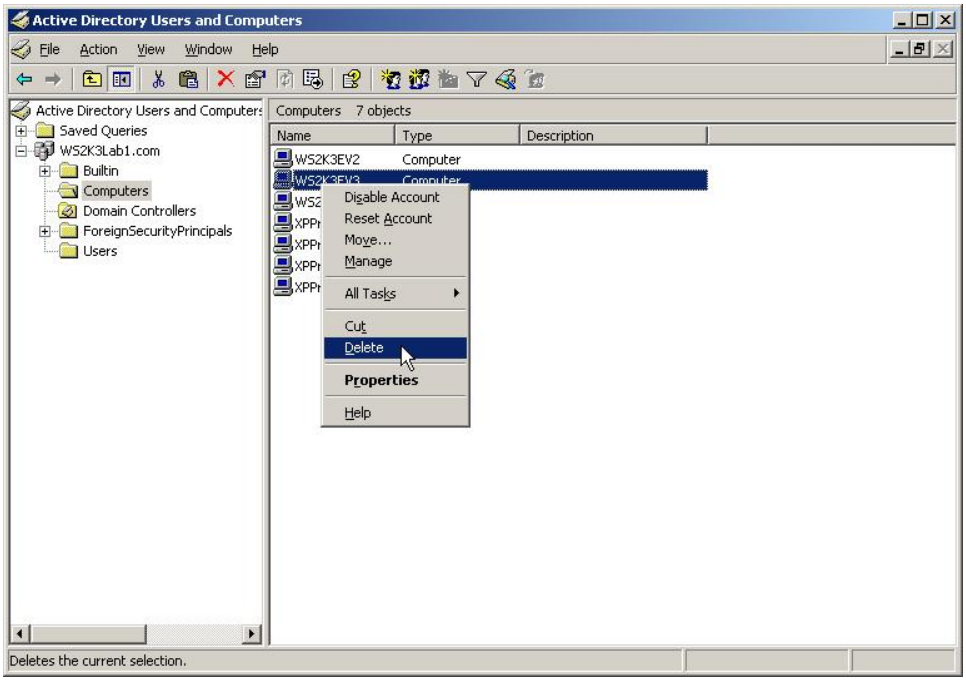
Locally, a computer can be removed from a domain by following the procedures in the Joining a computer to a Domain or Workgroup subsection to change the computers membership from a workgroup to a domain.

Use the following procedures to remotely remove a computer from a domain.

1. Log on to a Domain Controller using an authorized administrator account.
2. Open the Active Directory Users and Computers interface.
3. Select **Computers**. A list of computer objects will appear in the right hand pane.
4. Right-click on the computer to be removed and select **Delete** from the menu to remove the computer from the domain.

Copyright © 2008 Microsoft Corporation.

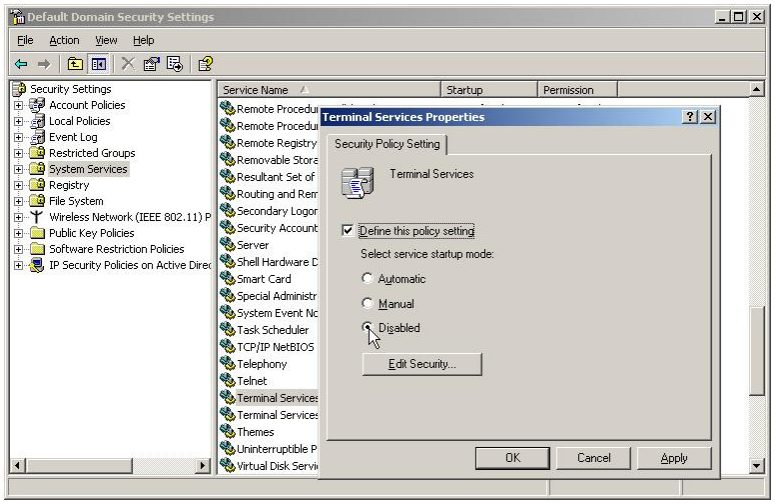
All rights reserved.



Disable Unnecessary System Services on Domain Computers

Use the following procedure to set a policy to disable unnecessary services within a domain or to set a policy to disable unnecessary services for Domain Controller:

1. Open the Domain Security Policy or the Domain Controller Security Policy as applicable.
2. Expand **Security Settings** and click on **System Services**.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Security**.
4. In the Security Policy Setting interface, check the Define this policy setting box and then select the **Disabled** radio button. Click the **OK** button.

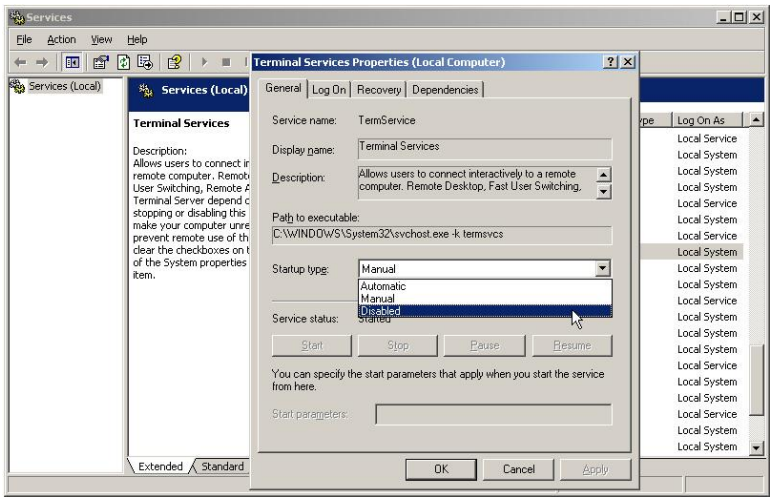


Copyright © 2008 Microsoft Corporation.
All rights reserved.

Disable Unnecessary System Services Locally

Use the following procedure to disable unnecessary services locally on Windows Server 2003:

1. Log on as an authorized administrator.
2. Click Start, point to Administrative Tools, and select Services.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Properties**.
4. The **Properties** interface for the selected service will appear. From the **Startup type:** drop down menu, select **Disabled**.



5. Under **Service status:** click on the **Stop** button.
6. Click the **OK** button.

Locking and Unlocking a User Desktop

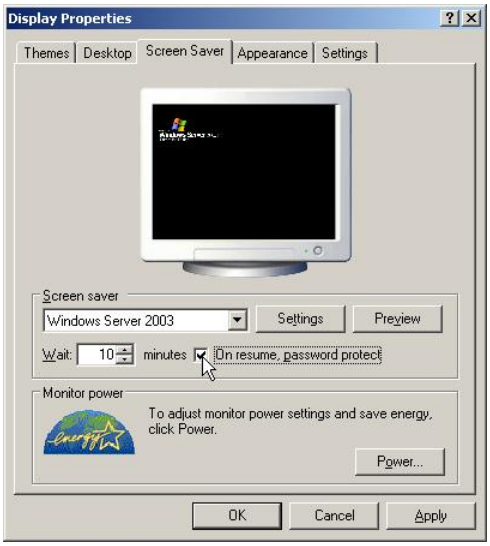
A user desktop may be locked for security reasons either by setting an automatic screen lock that is initiated with the screensaver after a set period of inactivity, or by manually choosing to lock the computer. Once the computer screen lock is invoked, access to the computer will only be allowed to the user whose account is currently logged on to the computer or by an authorized administrator.

Users may set an automatic screen lock on a workstation by setting screensaver based screen lock as follows:

1. Right click on the user desktop and select **Properties**. The **Display Properties** window will appear.
2. Click on the **Screen Saver** tab.
3. Select a screen saver from the **Screen Saver** drop down menu.
4. Enter the number of minutes of inactivity that the system must wait before initiating the screen saver in the **Wait**: text box. The default for Windows Server 2003 is 10 minutes.
5. Check the On resume, password protect check box.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

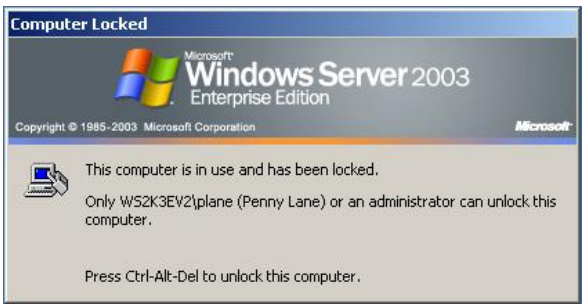


6. Click **OK** to set the password protected screen saver.

Users may manually initiate a screen lock as follows:

1. Simultaneously press the **Ctrl-Alt-Del** buttons. This will invoke the trusted path function an present the **Windows Security** interface.
2. Click on the **Lock Computer** button.

3. This will lock the users desktop, as indicated by the **Computer Locked** window.



A user can unlock the screen as follows:

1. Simultaneously press the **Ctrl-Alt-Del** buttons. This will invoke the trusted path function an present a login interface to unlock the computer.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. Enter the account name of the currently logged on user and the associated password.
3. Click **OK** to unlock the computer screen.

In the event emergency access is required to a user desktop that has been locked by either a screensaver based password lock or through a user-initiated action, an authorized administrator may unlock the computer screen as follows:

1. Simultaneously press the **Ctrl-Alt-Del** buttons. This will invoke the trusted path function an present a login interface to unlock the computer.
2. Enter the authorized administrator's account name and password and click **OK**.
3. A **Logon Message** will appear, warning that the current user will be logged off and any unsaved work will be lost. Click **OK** to log the current user off.

4. The current user gets logged off and the administrator or another authorized user may now log into the computer.

Managing Disk Quotas

Windows Server 2003 disk quotas track and control disk storage usage on a per-user, per-volume basis. Windows Server 2003 tracks disk quotas for each volume, even if the volumes are on the same hard disk. Because quotas are tracked on a per-user basis, every user's disk space is tracked regardless of the folders in which the user stores files.

The following list describes several important characteristics of Windows Server 2003 disk quotas.

- Windows Server 2003 calculates disk space usage for users based on the files and folders they own. When a user copies or saves a file to an NTFS volume or takes ownership of a file on an NTFS volume, Windows Server 2003 charges the disk space for the file against the user's quota limit.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Windows Server 2003 ignores compression when it calculates hard disk space usage. Users are charged for each uncompressed byte, regardless of how much hard disk space is actually used. In part, this charge is made because file compression produces different degrees of compression for different types of files. Different file types that are the same size when compressed might end up to be very different sizes when they are compressed.
- When disk quotas are enabled, the free disk space Windows Server 2003 reports to applications is the amount of space remaining within the user's disk quota limit. For example, a user whose files occupy 450 MBs of an assigned disk quota limit of 500 MBs will show 50 MBs of free space even if the volume contains several gigabytes of free space.

Disk quotas can be used to monitor and control hard disk space usage. System administrators can perform the following tasks:

- Set a disk quota limit to specify the amount of disk space for each user.
- Set a disk quota warning to specify when Windows Server 2003 should log an event, indicating that the user is nearing his or her limit.
- Enforce disk quota limits and either deny users access if they exceed their limit or allow them to continue access.
- Log an event when a user exceeds a specific disk space threshold. For example, a threshold might be when users exceed their quota limit or when they exceed their warning level.

After enabling disk quotas for a volume, Windows Server 2003 collects disk usage data for all users who own files and folders on the volume. This allows monitoring of volume usage on a per-user basis. By default, only members of the Administrators group can view and change the quota settings. However, the administrator can allow users to view quota settings.

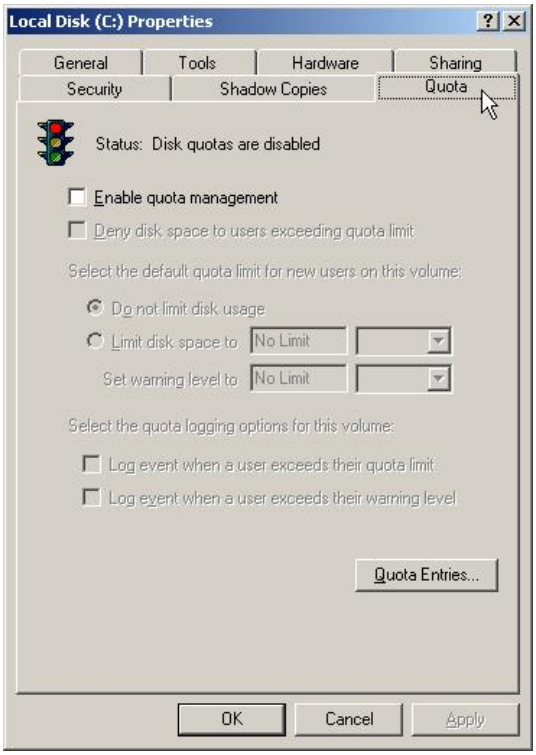
Setting Disk Quotas

Authorized administrators can enable disk quotas and enforce disk quota warnings and limits for all users or for individual users. To enable disk quotas:

1. Click **Start**, and select **My Computer**.
2. Right-click the disk volume for which disk quotas is to be enabled, and then click **Properties**. If the volumes are not formatted with the NTFS file system, or if the user is not a member of the Administrators group, the **Quota** tab is not displayed in the volume's Properties interface.
3. In the **Properties** interface, click the **Quota** tab.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

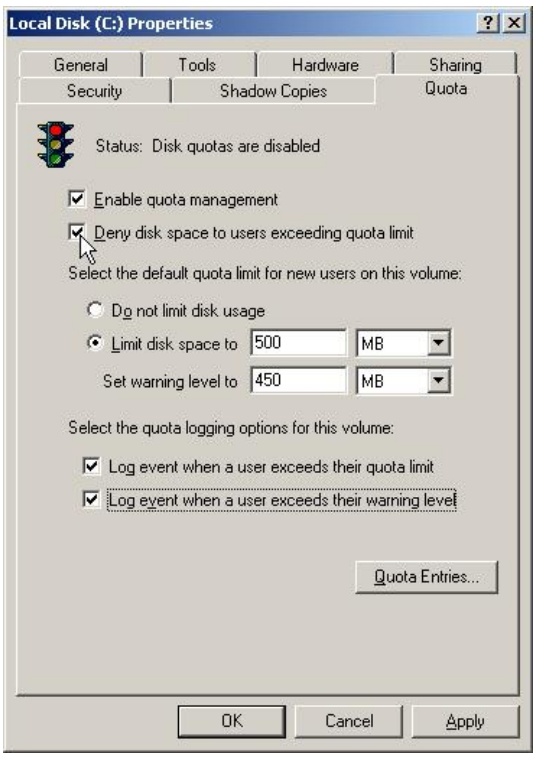


4. On the **Quota** properties page, click the **Enable quota management** check box, configure the disk quota options, and then click **OK**. The options on the **Quota** tab are described in the following table.

Option	Description
Enable Quota Management	Select this box to enable disk quota management.
Deny Disk Space To Users Exceeding Quota Limit	Select this box so that when users exceed their hard disk space allocation, they receive an "out of disk space" message and cannot write to the volume.
Do Not Limit Disk Usage	Click this option when it is not necessary to limit the amount of hard disk space for users.
Limit Disk Space To	Configure the amount of disk space that users can use.
Set Warning Level To	Configure the amount of disk space that a user can fill before Windows Server 2003 logs an event, indicating that a user is nearing his or her limit.
Quota Entries	Click this button to open the **Quota Entries** for an interface, where authorized administrators can add a new entry, delete an entry, and view the per-user quota information.

5. To enforce identical quota limits for all users, enter the appropriate values in the **Limit disk space to** text box and the **Set warning level to** text box, and then select the **Deny disk space to users exceeding quota limit** check box.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



Windows Server 2003 monitors usage and will not allow users to create files or folders on the volume when they reach the limit.

Determining the Status of Disk Quotas

Authorized administrators can determine the status of disk quotas in the **Properties** interface for a disk by checking the traffic light icon and reading the status message to its right. The traffic light colors and the status they indicate are as follows:

- A red traffic light indicates that disk quotas are disabled.
- A yellow traffic light indicates that Windows Server 2003 is rebuilding disk quota information.
- A green traffic light indicates that the disk quota system is active.

Monitor Disk Quotas

Authorized administrators can use the **Quota Entries For <*volume_name*>** interface to monitor usage for all users who have copied, saved, or taken ownership of files and folders on the volume. The **Quota Entries For <*volume_name*>** interface is accessed by pressing the **Quota Entries** button on the **Quota** tab of the volume **Properties** interface. Windows Server 2003 scans the volume and monitors the amount of disk space in use by each user. The **Quota Entries For <*volume_name*>** interface allows authorized administrators to view the following information:

- The amount of hard disk space that each user uses.
- Users who are over their quota-warning threshold, which is signified by a yellow triangle.
- Users who are over their quota limit, which is signified by a red circle.
- The warning threshold and the disk quota limit for each user.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Volume usage is tracked for all users owning files on a volume where the disk quota system is active. Existing users owning files are limited to the default disk quota unless authorized administrators modify the user quota setting using the **Quota Entries For <*volume_name*>** interface. User not owning files on the volume will not appear in the **Quota Entries For <*volume_name*>** interface but can also be added manually. By default, quota limits are not applied to the Administrators local group.

Exceeding Disk Quota Limits

When the **Deny disk space to users exceeding quota limit** option is selected, users who exceed their quota limit receive an "insufficient disk space" error from Windows and cannot write additional data to the volume without first deleting or moving some existing files from it.

Individual programs determine their own error handling for this condition. To the program, it appears that the volume is full. If this option is left cleared, users can exceed their quota limit. Enabling quotas and not limiting disk space use are useful when administrators do not want to deny users access to a volume, but want to track disk space use on a per-user basis. Authorized administrators can also specify whether or not to log an event when users exceed either their quota warning level or their quota limit.

When the **Log event when a user exceeds their quota limit** option is selected, an event is written to the Windows system log on the computer running disk quotas whenever users exceed their quota limit. Authorized administrators can view these events with Event Viewer, filtering for disk event types.

When the **Log event when a user exceeds their warning level** option is selected, an event is written to the Windows system log on the computer running disk quotas whenever users exceed their quota warning level. Authorized administrators can view these events with Event Viewer, filtering for disk event types. Unless a trigger is set to do so, users are not warned of this event.

To modify user disk space and warning levels:

1. Right-click the volume for which quota values are to be modified, and then click **Properties**.
2. In the **Properties** interface, click the **Quota** tab.
3. On the **Quota** properties page, click **Quota Entries**.
4. In the **Quota Entries** window, click the entries for the users whose options are to be modified, and on the **Quota** menu, click **Properties**.
5. In the **Quota Settings** interface, modify any of the following options that are to be changed, and then click **OK**:
   - **Do not limit disk usage**. Click to track disk space usage without limiting disk space.
   - **Limit disk space to**. Activates fields for limiting disk space and setting warning levels. Type a numeric value in the text field, and select a disk space limit unit from the drop-down list. Authorized administrators can use decimal values (for example, 100.5 MB). The value entered cannot exceed the maximum capacity of the volume.

To delete quota entries:

1. Right-click the volume for which quota entries are to be deleted, and then click **Properties**.
2. In the **Properties** interface, click the **Quota** tab.
3. On the **Quota** tab page, click **Quota Entries**.
4. In the **Quota Entries** window, click the entries for the users to be deleted, and then from the **Quota** menu, click **Delete quota entry**.
5. If the **Disk Quota** interface appears, click **Yes**, click the files to take action on, click one of the following buttons, and then click **Close**:
   - **Delete**. Deletes selected files from the volume.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Take ownership**. Gives ownership of selected files on the volume.
- **Move**. Moves selected files to a specified volume.

To disable disk quotas:

1. Right-click the disk volume for which disk quotas are to be disabled, and then click **Properties**.
2. In the **Properties** interface, click the **Quota** tab.
3. On the **Quota** tab, clear the **Enable quota management** check box, and then click **OK**.

Active Directory Sites and Services

Active Directory uses multi-master replication, enabling any Windows Server 2003 Domain Controller in the forest to service requests, including modifications to the directory by users.

If there is a small deployment of well-connected computers, arbitrary selection of a Domain Controller may not cause problems. However, a deployment that comprises a Wide Area Network (WAN) could be extraordinarily inefficient when, for example, users in Sydney attempt to authenticate to Domain Controllers in New York using a dial-up connection. Active Directory Sites and Services can improve the efficiency of directory services for most deployments through the use of sites.

Authorized administrators provide information about the physical structure of the network by publishing sites to Active Directory using Active Directory Sites and Services. Active Directory uses this information to determine how to replicate directory information and handle service requests.

A *site* represents a region of uniformly good network access, which can be interpreted as being generally equivalent to LAN connectivity. LAN connectivity assumes high, inexpensive bandwidth that allows similar and reliable network performance, regardless of which two computers in the site are communicating. This quality of connectivity does not indicate that all servers in the site must be on the same network segment nor that hop counts between all servers must be identical. Rather, it can be interpreted as the measure by which it is known that if a large amount of data needed to be copied from one server to another, it would not matter which servers were involved. If there is concern about such situations, consider creating another site.

Computers are assigned to sites based on their location in a subnet or in a set of well-connected subnets. Subnets provide a simple way to represent network groupings, much the same way that postal codes conveniently group mailing addresses. Subnets are formatted in terms that make it easy to post physical information about network connectivity to the directory. Having all computers in one or more well-connected subnets also reinforces the standard that all computers in a site must be well-connected, since computers in the same subnet typically have better connections than an arbitrary selection of computers on a network.

Sites facilitate:

- **Authentication**. When clients log on using a domain account, the logon mechanism first searches for Domain Controllers that are in the same site as the client. Attempting to use Domain Controllers in the client's site first localizes network traffic, increasing the efficiency of the authentication process.
- **Replication**. Directory information is replicated both within and among sites. Active Directory replicates information within a site more frequently than across sites. This balances the need for up-to-date directory information with the limitations imposed by available network bandwidth.

  Authorized administrators customize how Active Directory replicates information using site links to specify how the sites are connected. Active Directory uses the information about how sites are connected to generate Connection objects that provide efficient replication and fault tolerance.

  Authorized administrators provide information about the cost of a site link, times when the link is available for use and how often the link should be used. Active Directory uses this information to determine which site link will be used to replicate information. Customizing replication schedules so

Copyright © 2008 Microsoft Corporation.

All rights reserved.

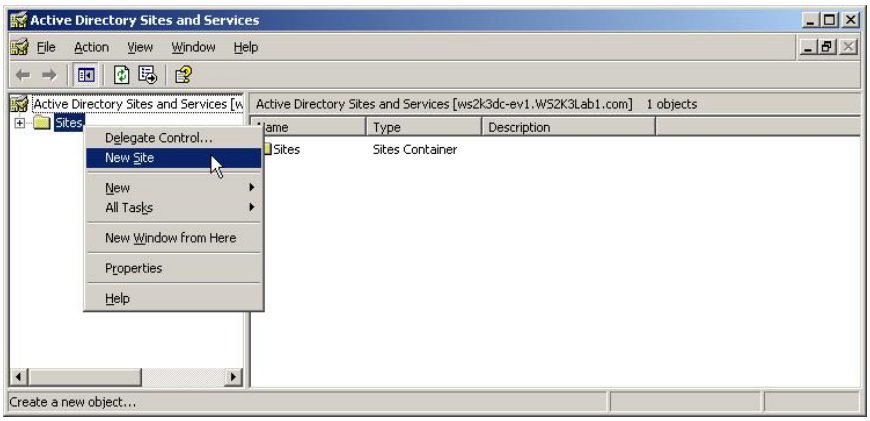
replication occurs during specific times, such as when network traffic is low, will make replication more efficient.

Ordinarily, all Domain Controllers are used to exchange information between sites, but authorized administrators can further control replication behavior by specifying a bridgehead server for inter-site replicated information. Establish a bridgehead server when there is a specific server to dedicate for inter-site replication, rather than using any server available. Authorized administrators can also establish a bridgehead server when the deployment uses proxy servers, such as for sending and receiving information through a firewall.

- **Active Directory enabled services**. Information such as service bindings and configurations can be made available through the directory, making administration and use of network resources easier and more efficient. Sites help structure and optimize distribution of service information, so the current information is available to clients and distributed efficiently throughout the network.

To create a site:

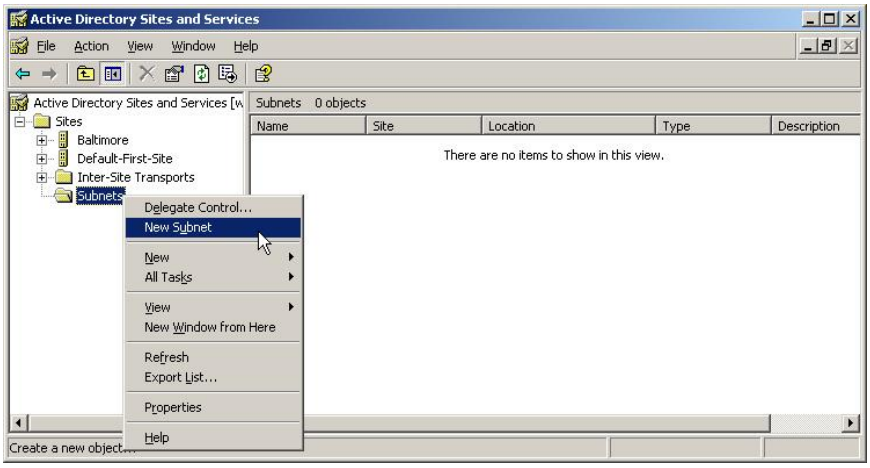
1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
2. Right-click the **Sites folder**, and then click **New Site**.



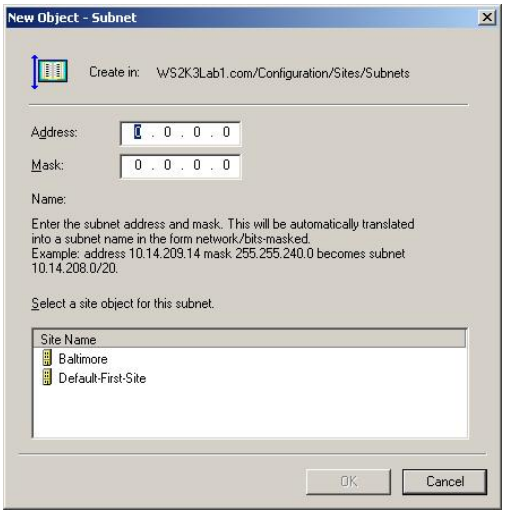
3. In **Name**, type the name of the new site
4. Click a site link object, and then click **OK**. The following message will appear. Click **OK**.

5. Associate a subnet with a site for this newly created site:
   - Expand **Sites**. Right-click on **Subnets** and select **New Subnet**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

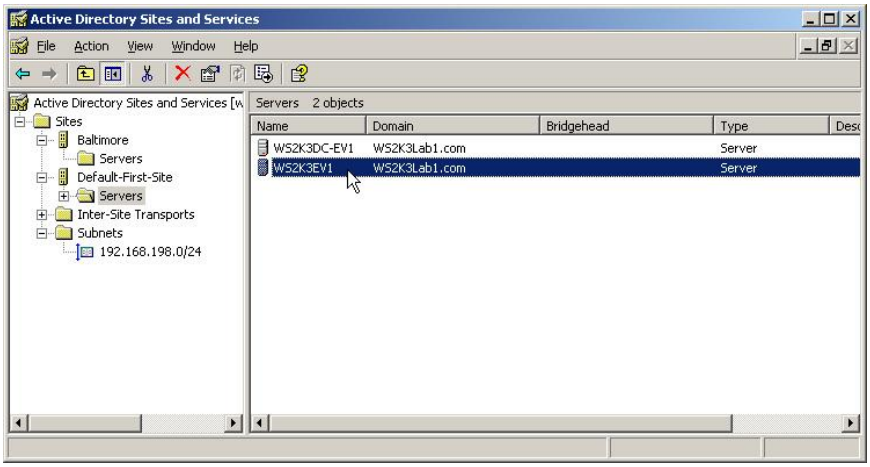


- In the **New Object – Subnet** interface, enter the subnet and mask, select the site for the subnet and click **OK**.



6. Move a Domain Controller from an existing site into this new site, or install a new Domain Controller:

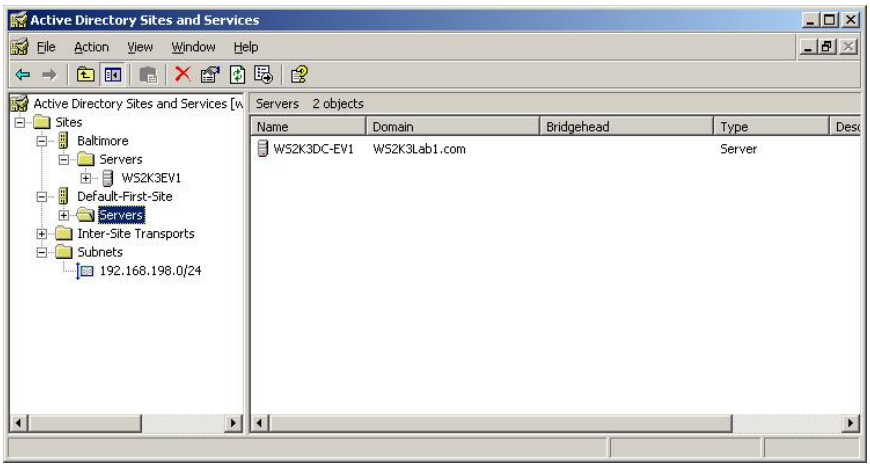
- Expand the site nodes. Select a server from an existing site's **Servers** folder and drag it to the new site's **Servers** folder.



- A warning message may appear. Read the message and click **Yes**, if it is OK to proceed.

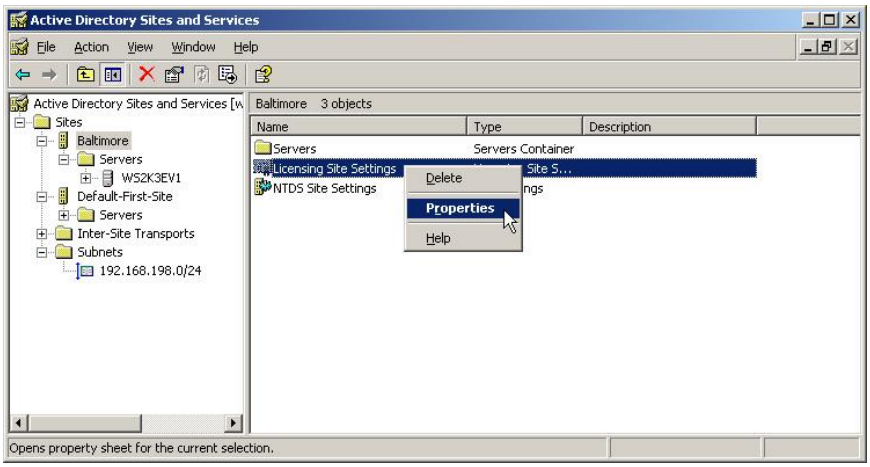
Copyright © 2008 Microsoft Corporation.
All rights reserved.

- The server will appear in the new site node.



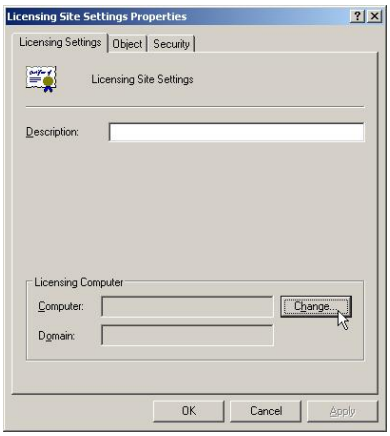
7. To choose a specific licensing computer, other than the one automatically selected, select another licensing computer:

   - Select the new site node. In the right-hand details pane, right-click on **Licensing Site Settings** and select **Properties**.



- In the Licensing Site Settings Properties interface, click the change button and select a computer.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

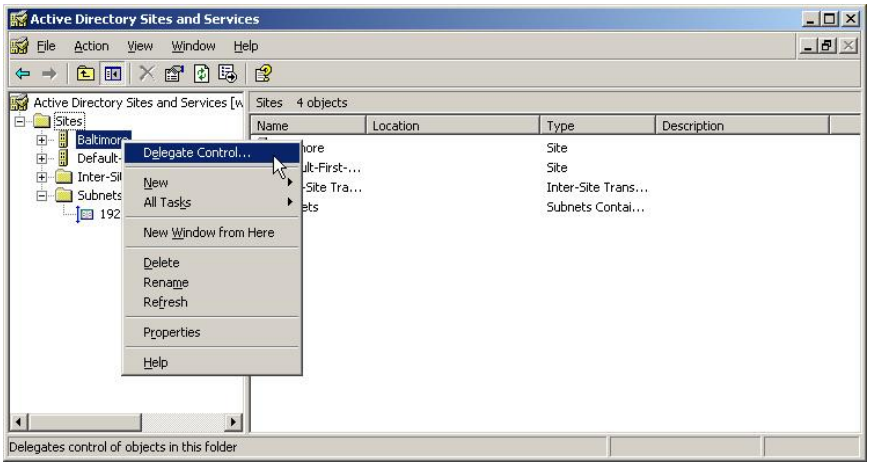


8. Delegate control of the site.

To Delegate Control

In **Active Directory Sites and Services**, authorized administrators can delegate control for the Subnets, Inter-site Transports, Sites, and Server containers. Delegating control of an object allows administrators to specify who has permissions to access or modify that object or its child objects.

1. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
2. Right-click the container whose control is to be delegated, and then click **Delegate Control** to start the **Delegation of Control Wizard**.



3. Click **Next** and follow the instructions in the **Delegation of Control Wizard**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Active Directory Replication

Active Directory is a distributed directory service that stores objects that represent real-world entities such as users, computers, services, and network resources. Objects in the directory are distributed among all DCsin a forest, and all Domain Controllers can be updated directly. Active Directory replication is the process by which the changes that originate on one Domain Controller are automatically transferred to other Domain Controllers that store the same data.

Active Directory Replication Model

The Active Directory replication model defines the mechanisms that allow directory updates to be transferred automatically between Domain Controllers to provide a seamless replication solution for the Active Directory distributed directory service.

> **Note:** This discussion of the replication model and related mechanisms for transferring directory data between Domain Controllers does not include the topic of replication topology. Replication topology is the set of connections that are generated by the KCC to enable replication to take place between Domain Controllers.

Active Directory is distributed by means of directory partitions. In addition to directory partitions that store forest-wide data, each Domain Controller stores a replica of a single domain directory partition, which contains data that is specific to one or more closely aligned business units-the users, computers, organizational units, and network resources that are managed by the same set of service and data administrators. Because each Domain Controller stores only one domain directory partition, Active Directory can scale to hundreds or thousands of domains storing millions of objects.

To efficiently synchronize data between Domain Controllers that store the same domain, Active Directory replication transfers updates according to directory partition. Each Domain Controller receives directory updates to the data that is stored in its domain only, as well as updates that are stored in the two directory partitions that store configuration and schema data for the forest.

> **Note:** In Windows Server 2003 forests, Domain Controllers can also store application directory partitions, which store application data that can be replicated to only the Domain Controllers that store the directory partition, irrespective of domain.

Active Directory replication manages the transfer of these updates to the appropriate Domain Controllers automatically, keeping domain data up-to-date among all Domain Controllers in the domain, regardless of location. In the process, allDCs in the forest are also updated with changes to forest-wide data.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Replication Model Components

To globally distribute the directory service, the Active Directory replication model incorporates the components in the following table.

Component	Description	Advantage
Mult-master replication	Every Domain Controller can receive originating updates to data for which it is authoritative, rather than having a single Domain Controller that receives all original updates (single-master replication, such as Windows NT 4.0 replication).	Provides fault tolerance, eliminating the dependency on a single DCto maintain directory operations.
Pull replication	Domain Controllers request (pull) changes rather than send (push) changes that might not be needed.	Reduces unnecessary network traffic.
Store-and-forward replication	Each Domain Controller communicates with a subset of Domain Controllers to transfer replication changes, rather than one Domain Controller being responsible for communicating with every other DCthat requires the change.	Balances the replication load among many Domain Controllers.
State-based replication	Each Domain Controller tracks the state of replication updates.	Conflicts and unnecessary replication are reduced.

The Active Directory replication model ensures:

- **Domain Controller availability**. Multimaster replication ensures that all Domain Controllers are available for updates, eliminating the potential for slow service if only a single updatable Domain Controllers were available.
- **Efficient transfer of data**. State-based and pull replication ensures the minimum replication traffic and the maximum efficiency to retrieve only the changes that are needed.
- **Reliable consistency**. Directory consistency is guaranteed within the same period of replication latency.
- **Conflict resolution**. Even if two administrators change the same attribute on different Domain Controllers at the same time, conflict resolution ensures that only one of the values is replicated to all Domain Controllers.

Replication Latency

Multi-master replication involves *latency* — the period of time for an update that occurs on the originating Domain Controller to reach all other Domain Controllers that need it. To address replication latency, multi-master replication ensures *loose consistency* with *convergence*, as follows:

- Loose consistency means that the replicas are not guaranteed to be consistent with each other at any particular point in time because changes can originate from any replica at any time.
- Convergence means that if the system is allowed to reach a steady state in which no new updates are occurring and all previous updates have been completely replicated, all replicas of the same directory partition are guaranteed to converge on the same set of values.

With multi-master replication, it is not necessary for every Domain Controller to replicate with every other Domain Controller. Instead, the system implements a robust set of connections that determines which Domain Controllers replicate to which other Domain Controllers to ensure that networks are not overloaded with replication traffic and that replication latency is not so long that it inconveniences users.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The set of connections through which changes are replicated to Domain Controllers in an enterprise is called the replication topology.

Although it involves latency, multi-master update capability provides high availability of write access to directory objects because several servers can contain writable copies of an object. Each Domain Controller in the domain can accept updates independently, without communicating with other Domain Controllers. Active Directory replication resolves any conflicts that occur when multiple updates are made to a single directory object.

State-based vs. log-based Replication

In state-based replication, each Domain Controller (master) in the multimaster system applies updates to its replica as they arrive, without maintaining a change log file. In a typical log-based replication system (also called "change-based"), each master keeps a log of the updates that it originated and communicates its log to every other replica. After a log has arrived at a replica, the replica applies the log, bringing itself more up-to-date. In this process, the destination receives and stores a record of all changes, not just the changes it needs.

Active Directory replication relies on the current "state" (the current values of all objects) of the source replica instead of logs. The current state includes metadata that is used to resolve conflicts and to avoid sending the full replica on each replication cycle.

Generally speaking, a directory partition replica maintains all of its objects in a list ordered by last modification. This list is a log of sorts, but one whose size is a tiny fraction of the size of the replica itself. A typical replication request can be satisfied by examining only the last few objects on the list because the replication destination server is aware of how much of its replication source's list of changes have already been processed.

Multimaster vs. Single-master Replication

Although a single-master model is adequate for a directory that has a small number of replicas and for an environment where all of the changes can be applied centrally, this approach does not scale beyond small organizations nor does it address the needs of decentralized organizations.

Multi-master replication provides the following advantages over single-master replication:

- If one Domain Controller becomes inoperable, other Domain Controllers can continue to update the directory. In single-master replication, if the master becomes inoperable, directory updates cannot take place. For example, if the failed server holds a user's password and the password has expired, the user cannot reset the password and therefore cannot log on to the domain.
- Servers that are capable of making changes to the directory can be distributed across the network and can be deployed in multiple locations.
- By creating multiple replicas of the directory and keeping the replicas consistent, the directory service can handle more queries per second. Directory services must handle a large number of queries compared to the number of updates they must process. A typical ratio of queries to updates is 99:1.

Pull vs. Push Replication

In push replication, a source Domain Controller sends unsolicited information to update a destination Domain Controller. Push replication is problematic because it is difficult for the source to know what information the destination needs. The destination can receive the same information from another source. Therefore, a source can send unnecessary information to a destination.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Active Directory Replication Dependencies

Active Directory replication has the following dependencies:

- **DNS.** The DNS that resolves DNS names to IP addresses. Active Directory requires that DNS is properly designed and deployed so that Domain Controllers can correctly resolve DNS names of replication partners.
- **RPC**. Active Directory replication requires IP connectivity and the RPC to transfer updates between replication partners.
- **Kerberos v5 Authentication**. The authentication protocol for both authentication and encryption that is required for all Active Directory RPC replication.
- **LDAP Protocol**. The primary access protocol for Active Directory. Replication of an entire replica of an Active Directory domain, as occurs when Active Directory is installed on an additional Domain Controller in an existing domain, uses LDAP communication rather than RPC.

Active Directory Replication Topology

Replication of updates to Active Directory objects are transmitted between multiple Domain Controllers to keep replicas of directory partitions synchronized. Multiple domains are common in large organizations, as are multiple sites in disparate locations. In addition, Domain Controllers for the same domain are commonly placed in more than one site.

Therefore, replication must often occur both within sites and between sites to keep domain and forest data consistent among Domain Controllers that store the same directory partitions. Site objects can be configured to include a set of subnets that provide LAN network speeds. As such, replication within sites generally occurs at high speeds between Domain Controllers that are on the same network segment. Similarly, site link objects can be configured to represent the WAN links that connect LANs. Replication between sites usually occurs over these WAN links, which might be costly in terms of bandwidth. To accommodate the differences in distance and cost of replication within a site and replication between sites, the intra-site replication topology is created to optimize speed, and the inter-site replication topology is created to minimize cost.

The KCC is a distributed application that runs on every Domain Controller and is responsible for creating the connections between Domain Controllers that collectively form the replication topology. The KCC uses Active Directory data to determine where (from what source Domain Controller to what destination Domain Controller) to create these connections.

Replication Within and Between Sites

The KCC creates separate replication topologies to transfer Active Directory updates within a site and between all configured sites in the forest. The connections that are used for replication within sites are created automatically with no additional configuration. Intra-site replication takes advantage of LAN network speeds by providing replication as soon as changes occur, without the overhead of data compression, thus maximizing Central Processing Unit (CPU) efficiency. Intra-site replication connections form a ring topology with extra shortcut connections where needed to decrease latency. The fast replication of updates within sites facilitates timely updates of domain data. In deployments where large datacenters constitute hub sites for the centralization of mission-critical operations, directory consistency is critical.

Replication between sites is made possible by user-defined site and site link objects that are created in Active Directory to represent the physical LAN and WAN network infrastructure. When Active Directory sites and site links are configured, the KCC creates an inter-site topology so that replication flows between Domain Controllers across WAN links. Inter-site replication occurs according to a site link schedule so that WAN usage can be controlled, and is compressed to reduce network bandwidth requirements. Site

Copyright © 2008 Microsoft Corporation.

All rights reserved.

link settings can be managed to optimize replication routing over WAN links. The connections that are created between sites form a spanning tree for each directory partition in the forest, merging where common directory partitions can be replicated over the same connection.

In remote branch locations, replication of updates from the hub sites is optimized for network availability. Thus, because intra-site replication is optimized for speed, branch locations across WAN links can be assured of receiving data from hub sites that is up-to-date and reliable; but because inter-site replication is scheduled, branch sites receive this replication only at intervals that are deemed appropriate and cost-effective for remote operations.

Technologies Related to Active Directory Replication Topology

The following technologies interact with Active Directory replication.

- **FRS.** FRS is related to Active Directory replication because it requires the Active Directory replication topology. FRS is a multimaster replication service that is used to replicate files and folders in the System Volume (SYSVOL) shared folder on Domain Controllers and in DFS shared folders. FRS works by detecting changes to files and folders and then replicating the updated files and folders to other replica members, which are connected in a replication topology.

  FRS uses the replication topology that is generated by the KCC to replicate the SYSVOL files to all Domain Controllers in the domain. SYSVOL files are required by all Domain Controllers for Active Directory to function.

- **Simple Mail Transfer Protocol (SMTP).** SMTP is a packaging protocol that can be used as an alternative to the RPC replication transport. SMTP can be used to transport non-domain replication over IP networks in mail-message format. Where networks are not fully routed, e-mail is sometimes the only transport method available.

  Note: SMTP is not included in the Evaluated Configuration.

Active Directory Replication Topology Dependencies

Active Directory replication topology has the following dependencies:

- **Routable IP infrastructure.** The replication topology is dependent upon a routable IP infrastructure from which IP subnet address ranges can be mapped to site objects. This mapping generates the information that is used by client workstations to communicate with Domain Controllers that are close by, when there is a choice, rather than those that are located across WAN links.

- **DNS.** The DNS resolves DNS names to IP addresses. Active Directory replication topology requires that DNS is properly designed and deployed so that Domain Controllers can correctly resolve the DNS names of replication partners.

  DNS also stores service resource records that provide site affinity information to clients searching for Domain Controllers, including Domain Controllers that are searching for replication partners. Every Domain Controller registers these records so that they can be located according to site.

- **Net Logon Service.** Net Logon is required for DNS registrations.

- **RPC.** Active Directory replication requires IP connectivity and RPC to transfer updates between replication partners within sites. RPC is required for replication between two sites containing Domain Controllers in the same domain, but SMTP is an alternative where RPC cannot be used and Domain Controllers for the same domain are all located in one site so that inter-site replication of domain data is not required.

  Note: SMTP is not part of the Evaluated Configuration.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Intersite Messaging.** Inter-site Messaging is required for SMTP inter-site replication and for site coverage calculations.

How replication Works

To keep directory data on all Domain Controllers consistent and up to date, Active Directory replicates directory changes on a regular basis. Replication occurs over standard network protocols, uses change tracking information to prevent unnecessary replication, and uses linked value replication to improve efficiency.

Transferring Replication Data

Active Directory uses RPC over IP to transfer replication data between Domain Controllers. RPC over IP is used for both intersite and intrasite replication. To keep data secure while in transit, RPC over IP replication uses both authentication (using the Kerberos V5 authentication protocol) and data encryption.

When a direct or reliable IP connection is not available, replication between sites can be configured to use the SMTP. However, SMTP replication functionality is limited, and requires an enterprise CA. SMTP can only be used to replicate the configuration, schema and application directory partitions, and does not support the replication of domain directory partitions.

Note: SMTP is not part of the Evaluated Configuration.

Preventing Unnecessary Replication

Once a Domain Controller has processed a directory change from another Domain Controller successfully, it should not try to replicate those changes back to the Domain Controller that sent the change. In addition, a Domain Controller should avoid sending updates to another Domain Controller if the target Domain Controller has already received that same update from a different replication partner. To prevent such unnecessary replication, Active Directory uses change tracking information stored in the directory.

Resolving Conflicting Changes

It is possible for two different users to make changes to the exact same object property and to have these changes applied at two different Domain Controllers in the same domain before replication of either change occurs. In such a case, both changes are replicated as new changes, creating a conflict. To resolve this conflict, Domain Controllers that receive these conflicting changes examine the attribute data contained within the changes, each of which holds a version and a timestamp. Domain Controllers will accept the change with the higher version and discard the other change. If the versions are identical, Domain Controllers will accept the change with the more recent timestamp.

Improving Replication Efficiency

Introduced in the Windows Server 2003 family, linked value replication allows individual values of a multi-valued attribute to be replicated separately. In Windows 2000, when a change was made to a member of a group (one example of a mult-ivalued attribute with linked values) the entire group had to be replicated. With linked value replication, only the group member that has changed is replicated, and not the entire group. To enable linked value replication, the forest functional level must be raised to Windows Server 2003.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Replication Within a Site

Active Directory handles replication within a site, or intra-site replication, differently than replication between sites because bandwidth within a site is more readily available. The Active Directory KCC builds the intra-site replication topology using a bidirectional ring design. Intra-site replication is optimized for speed, and directory updates within a site occur automatically on the basis of change notification. Unlike replication data traveling between sites, directory updates replicated within a site are not compressed.

Building the Intra-site Replication Topology

The KCC on each Domain Controller automatically builds the most efficient replication topology for intrasite replication, using a bidirectional ring design. This bidirectional ring topology attempts to create at least two connections to each Domain Controller (for fault tolerance) and no more than three hops between any two Domain Controllers (to reduce replication latency). To prevent connections of more than three hops, the topology can include shortcut connections across the ring. The KCC updates the replication topology regularly.

Note: The KCC actually creates a separate replication topology for each directory partition (schema, configuration, domain, application). Within a single site, these topologies are usually identical for all partitions hosted by the same set of the Domain Controllers.

Determining when Intra-site Replication Occurs

Directory updates made within a site are likely to have the most direct impact on local clients, so intra-site replication is optimized for speed. Replication within a site occurs automatically on the basis of change notification. Intra-site replication begins when a directory update is made on a Domain Controller. By default, the source Domain Controller waits 15 seconds and then sends an update notification to its closest replication partner. If the source Domain Controller has more than one replication partner, subsequent notifications go out by default at three (3) second intervals to each partner. After receiving notification of a change, a partner Domain Controller sends a directory update request to the source Domain Controller. The source Domain Controller responds to the request with a replication operation. The three (3) second notification interval prevents the source Domain Controller from being overwhelmed with simultaneous update requests from its replication partners.

For some directory updates in a site, the 15 second waiting time does not apply and replication occurs immediately. Known as urgent replication, this immediate replication applies to critical directory updates, including the assigning of account lockouts and changes in the account lockout policy, the domain password policy, or the password on a Domain Controller account.

Replication between Sites

Active Directory handles replication between sites, or inter-site replication, differently than replication within sites because bandwidth between sites is usually limited. The Active Directory KCC builds the intersite replication topology using a least-cost spanning tree design. Inter-site replication is optimized for bandwidth efficiency, and directory updates between sites occur automatically based on a configurable schedule. Directory updates replicated between sites are compressed to preserve bandwidth.

Building the Inter-site Replication Topology

Active Directory automatically builds the most efficient inter-site replication topology using information provides (through Active Directory Sites and Services) about the site connections. The directory stores this information as site link objects. One Domain Controller per site, called the inter-site topology

Copyright © 2008 Microsoft Corporation.

All rights reserved.

generator, is assigned to build the topology. A least-cost spanning tree algorithm is used to eliminate redundant replication paths between sites. The inter-site replication topology is updated regularly to respond to any changes that occur in the network. Authorized administrators can control inter-site replication through the information provided when the site links were created.

Determining when Inter-site Replication Occurs

Active Directory preserves bandwidth between sites by minimizing the frequency of replication and by allowing authorized administrators to schedule the availability of site links for replication. By default, inter-site replication across each site link occurs every 180 minutes (three (3) hours). The frequency can be adjusted to match an organization's specific needs. Be aware that increasing this frequency increases the amount of bandwidth used by replication. In addition, the availability of site links can be scheduled for use by replication. By default, a site link is available to carry replication traffic 24 hours a day, seven (7) days a week. This schedule can be limited to specific days of the week and times of day. For example, inter-site replication can be scheduled so that it only occurs after normal business hours.

When to Establish a Single or Separate Sites

Authorized administrators can optimize the replication efficiency and reduce the administrative overhead of the network by establishing sites appropriately. The most effective number of sites depends on the physical design of the network. When a new forest is first created, a single, default Active Directory site (called Default-Site-First-Name) is created that represents the entire network. A forest or domain consisting of a single site can be very efficient for a single location network connected completely by high-speed bandwidth. If the forest or domain contains multiple geographic locations that communicate over low-speed WAN connections, establishing multiple sites provides more granular control of replication behavior, reduces authentication latency, and reduces network traffic on the WAN.

Why Bandwidth is Important

Within a site, bandwidth affects how efficiently replication can work. The frequency with which intra-site replication occurs requires high-speed bandwidth to function most effectively. So before creating new site, make sure that high-speed bandwidth connects all computers within the site candidate. Any area where Domain Controllers are connected by 10 Megabits Per Second (Mbps) or more of bandwidth is a good site candidate.

When to Establish a Single Site

If a network is comprised of a single LAN consisting of a single subnet, or if the network contains multiple subnets connected by a high-speed backbone, establishing a single site replication topology can provide the following benefits:

- Simplified replication management
- Prompt directory updates between all Domain Controllers

A single site topology allows all replication on a network to occur as intra-site replication, which requires no manual replication configuration. A single site design also allows all Domain Controllers to remain very current with respect to directory changes, because directory updates are replicated almost immediately.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

When to Establish Multiple Sites

When the network consists of multiple geographic locations connected by a WAN, establishing separate sites for each location provides the following benefits:

- Efficient use of WAN bandwidth for replication
- Granular control of replication behavior
- Reduction in authentication latency

Physically separate network locations typically communicate over WAN connections, which are most often characterized by low-speed bandwidth. By creating a separate site for each physical location on the network, administrators can ensure that Domain Controllers communicating over WAN connections use intersite replication, which is specifically designed for efficiency on low bandwidth connections.

With multiple sites, there is more granular control of replication behavior through several configurable inter-site replication settings. These settings include the relative cost of different replication paths, the Domain Controllers associated with each site, the subnets associated with each site, the frequency of directory update transfers, and the availability of connections for use by replication.

A network client logging on to a domain must contact a Domain Controller as part of the authentication process, first looking within its own site. If the site includes two or more physically separate network locations, the client may authenticate against a Domain Controller across a WAN connection. Authentication across a WAN introduces a delay in the authentication process. By placing physically separate network locations into separate Active Directory sites, administrators can ensure that clients first attempt to authenticate against a Domain Controller in their own site.

Managing Replication

Active Directory relies on site configuration information to manage and optimize the process of replication. Active Directory provides automatic configuration of these settings in some cases. In addition, authorized administrators can configure site-related information for a network using Active Directory Sites and Services. Configurable information includes settings for site links, site link bridges, and bridgehead servers.

Creating and Deleting Site Links

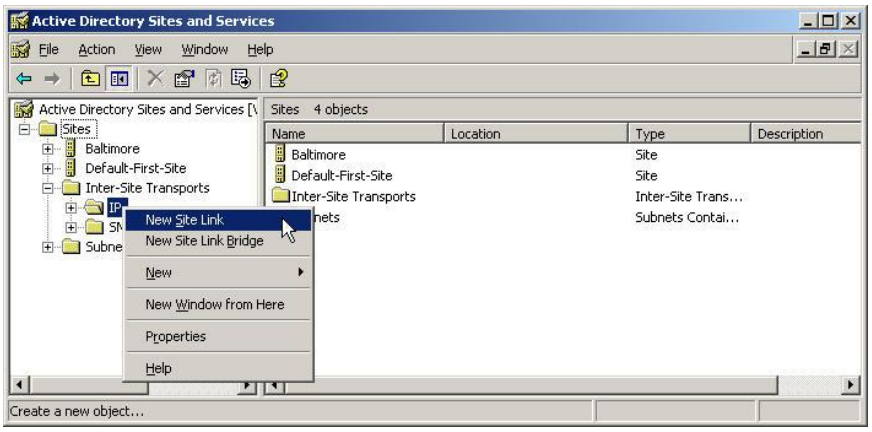
Creating a site link between two or more sites is a way to influence replication topology. By creating a site link, Active Directory is provided with information about what connections are available, which ones are preferred, and how much bandwidth is available. Active Directory uses this information to choose times and connections for replication that will afford the best performance.

To create a site link:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. Right-click the intersite transport protocol to be used by the site link, and then click **New Site Link**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

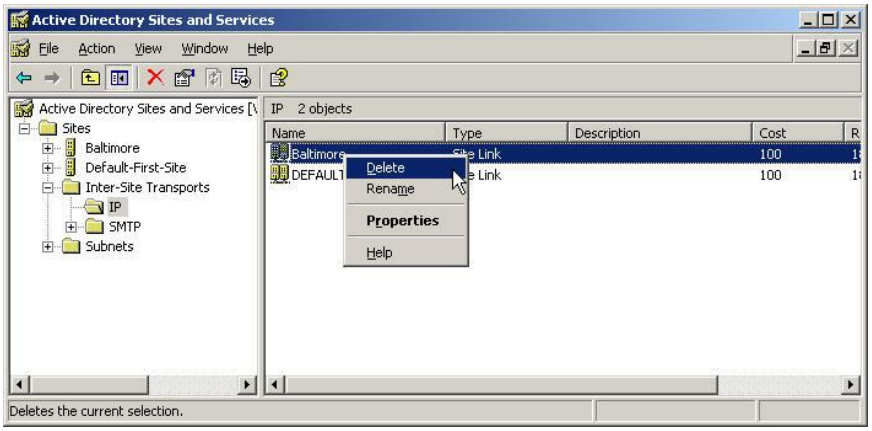


5. In **Name**, type the name to be given to the link.
6. Click two or more sites to connect, and then click **Add**.
7. Configure the site link's cost, schedule, and replication frequency. See related procedures below.

Note: If a site link is created that uses SMTP, an enterprise certification authority (Enterprise CA) must be available and SMTP must be installed on all Domain Controllers that will use the site link. SMTP is not included in the Evaluated Configuration.

To delete a site link:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, select the **Inter-Site Transports** subfolder that contains the site link to be deleted.
5. In the details pane, right-click the site link to be deleted, and then select **Delete**.



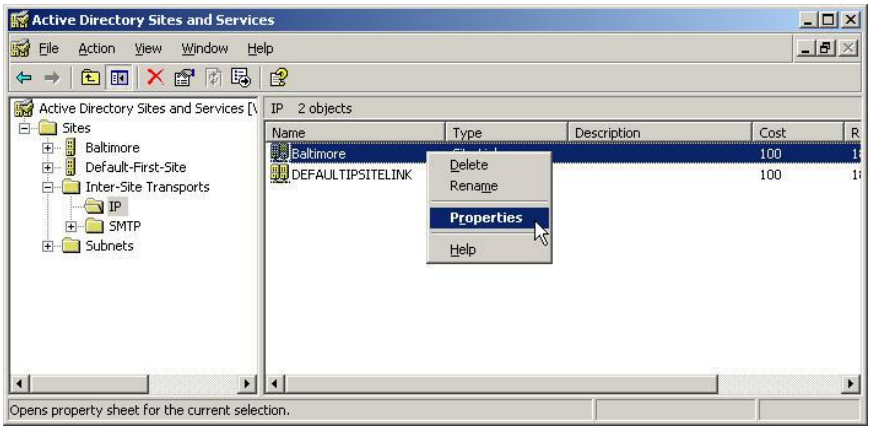
Note: Before deleting a site link, ensure that its member sites will still belong to at least one existing site link.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Adding a Site to a Site Link

To add a site to a site link:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, select the **Inter-Site Transports** subfolder that contains the site link where the site will be added.
5. In the details pane, right-click the site link and then select **Properties**.



6. Click the site to add to this site link from the **Sites not in this site link** box, and then click **Add**.
7. Close the site link **Properties** interface.

Creating and Deleting a Site Link Bridge

A site link bridge creates a chain of site links across which Domain Controllers from different sites in the site links can directly communicate.

By default, all site links are bridged, or transitive. This allows any two sites that are not connected by an explicit site link to communicate directly, through a chain of intermediary site links and sites. One advantage to bridging all site links is that the network is easier to maintain because it is not necessary to create a site link to describe every possible path between pairs of sites.

Generally, automatic site link bridging can be left enabled. However, it may be desirable to disable automatic site link bridging and create site link bridges manually just for specific site links, in the following cases:

- The network is not fully routed (not every Domain Controller can directly communicate with every other Domain Controller).
- There is a network routing or security policy in place that prevents every Domain Controller from being able to directly communicate with every other Domain Controller.
- The Active Directory design includes a large number of sites.

Copyright © 2008 Microsoft Corporation.

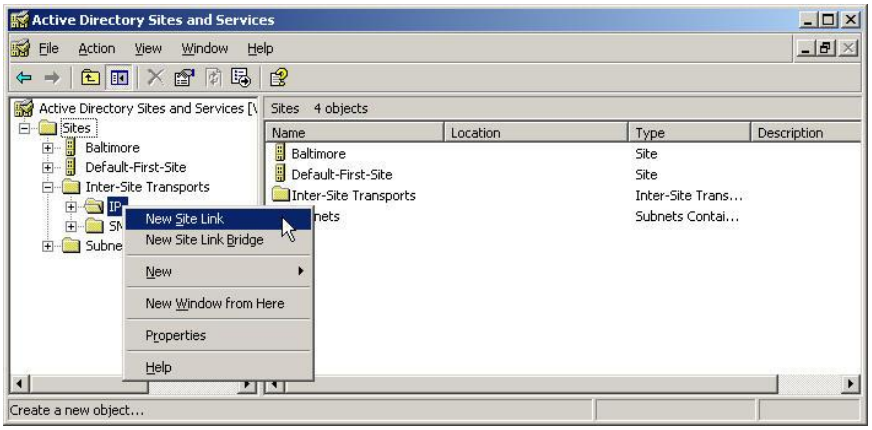
All rights reserved.

To create a site link bridge:

Note: If **Bridge all site links** is enabled (default setting), this procedure is redundant and will have no effect.

---

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, right-click the **Inter-Site Transports** subfolder where a new site link bridge is to be created, and then select **New Site Link Bridge**.



5. In **Name**, type a name for the site link bridge.
6. Click two or more site links to be bridged, and then click **Add**.

To delete a site link bridge:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, select the **Inter-Site Transports** subfolder that contains the site link bridge to be deleted.
5. In the details pane, right-click the site link bridge to be deleted, and then select **Delete**.

Enabling and Disabling a Site Link Bridge

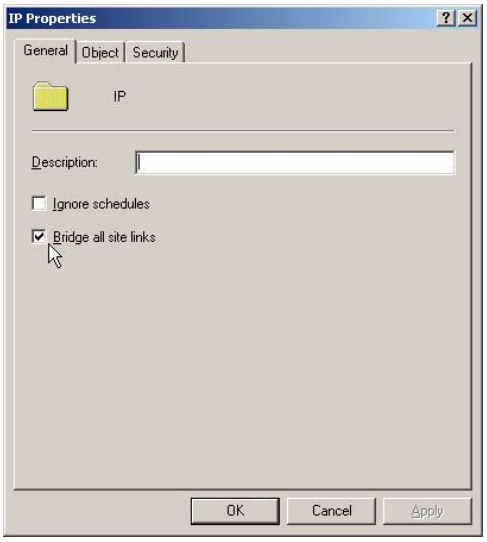
To enable or disable site link bridges:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, right-click the **Inter-Site Transports** subfolder (such as IP or SMTP) for which site link bridges are to be enabled or disabled, and then select **Properties**.
5. Do one of the following:
   - To enable site link bridges, select the **Bridge all site links** check box.
   - To disable site link bridges, clear the **Bridge all site links** check box.



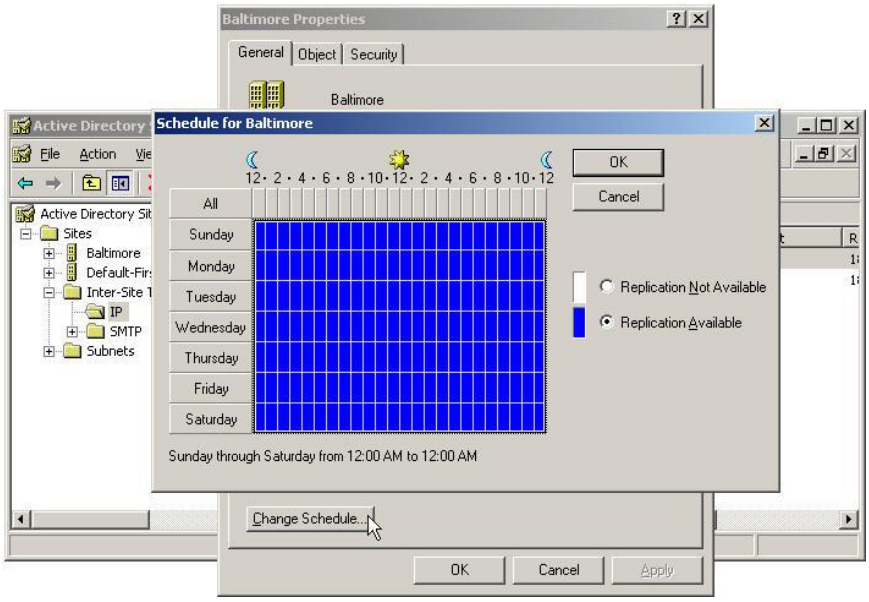
Configuring Site Link Replication Availability

The availability schedule for a site link determines during which hours or days of the week a site link can be used for replication. By default, a site link is always available for replication, 24 hours a day and seven (7) days a week. This schedule can be changed, for example, to exclude business hours during which the network is busy handling other types of traffic. Particular days, on which replication is not desired, can also be excluded.

To configure site link replication availability:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, select the **Inter-Site Transports** subfolder that contains the site link whose schedule is to be adjusted.
5. In the details pane, right-click the site link whose schedule to adjust, and then select **Properties**.
6. Click **Change Schedule**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



7. Select the block of time to be scheduled, and then click **Replication Not Available** or **Replication Available**.

Note: Replication availability schedules can be temporarily ignored by selecting **Ignore schedules** on the appropriate inter-site transport folder.

When **Ignore schedules** is selected, any site link availability schedules that have been configured are ignored, and all site links become always available for replication. When **Ignore schedules** is cleared, any previously configured site link availability schedules go back into effect. If no site link availability schedules have been configured, selecting **Ignore schedules** has no effect.

To ignore replication schedules:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, right-click the inter-site transport protocol that contains the site link schedules to be ignored, and then select **Properties**.
5. Select the **Ignore schedules** check box.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Configuring Site Link Cost

The Active Directory KCC considers a site link with a higher cost to be less desirable than a site link with a lower cost. When multiple paths for replication are available, the KCC prefers the site link with the lower cost.

To configure site link cost:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, select the **Inter-Site Transports** subfolder that contains the type of link to be configured.
5. In the details pane, right-click the site link whose cost is to be set, and then select **Properties**.
6. In **Cost**, enter a value for the cost of replication.

Note: Costs cannot be applied directly to site link bridges.

Configuring Site Link Replication Frequency

The replication frequency of a site link determines how often replication occurs over that site link. By default, the replication frequency for a site link is 180 minutes, meaning that replication occurs over that site link every 180 minutes, or three (3) hours. Using Active Directory Sites and Services, the replication frequency can be set from 15 minutes to 10,080 minutes (one week). A site link must be available for any replication to occur. If a site link is not available when the number of minutes between replication updates has passed, no replication will occur.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

To configure site link replication frequency:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, and then expand the **Inter-Site Transports** folder.
4. In the console tree, select the **Inter-Site Transports** subfolder that contains the site link to be configured.
5. In the details pane, right-click the site link whose replication frequency is to be set, and then select **Properties**.
6. In **Replicate every**, type the number of minutes between replications.

Forcing Replication over a Connection

To force replication over a connection:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, expand the site node, expand the **Servers** folder, and then expand the node for the server on which replication is to be forced.
4. In the console tree, select **NTDS Settings** for the server on which replication is to be forced.
5. In the details pane, right-click the connection over which to replicate directory information, and then select **Replicate Now**.

Manually Adding Connections

To manually add connections:

1. Log on as an authorized administrator that is a member of the Domain Admins group (in the forest root domain) or the Enterprise Admins group in Active Directory, or has been delegated the appropriate authority.
2. Click **Start**, point to **Administrative Tools**, and then select **Active Directory Sites and Services**.
3. Expand the **Sites** folder, expand the site node, expand the **Servers** folder, and then expand the node for the server on which an Active Directory connection is to be added.
4. In the console tree, right-click **NTDS Settings** for the Domain Controller on which to manually add a connection, and then click **New Active Directory Connection**.
5. In the **Find Domain Controllers** dialog box, select the Domain Controller that to be included in the connection object.
6. In the **New Object-Connection** dialog box, type a name for the new connection object.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: Active Directory automatically creates and deletes connection objects under normal conditions. If it is certain that a connection is required and that it is necessary for it to persist until it is manually removed, create a connection manually.

Protection of TSF

Set the Date and Time

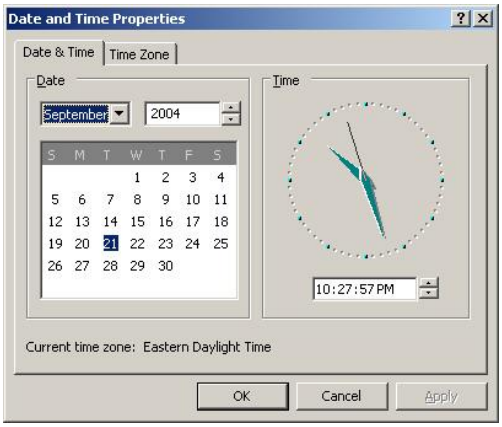
Computer time settings are set during the setup process, but can be changed by the administrator at any time through the **Date/Time Properties** GUI.

Setting the Date and Time during Setup

1. During Setup, in the **Date and Time Settings** interface, set the date, time, and time zone.
2. For the system to automatically adjust for daylight saving time, select the **Automatically adjust clock for daylight saving changes** check box.
3. Continue with Setup.

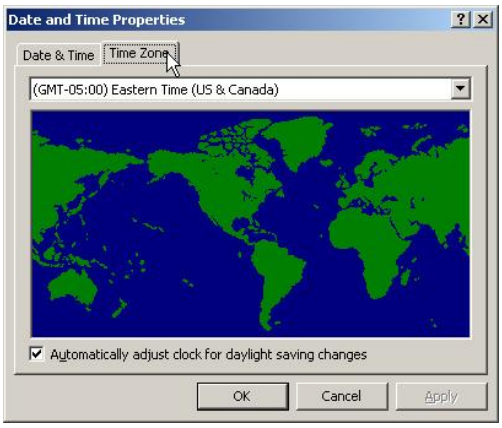
Setting the Date and On a Configured Computer

1. Open the **Date and Time Properties** Interface by double clicking on the clock display in the right corner of the task bar.

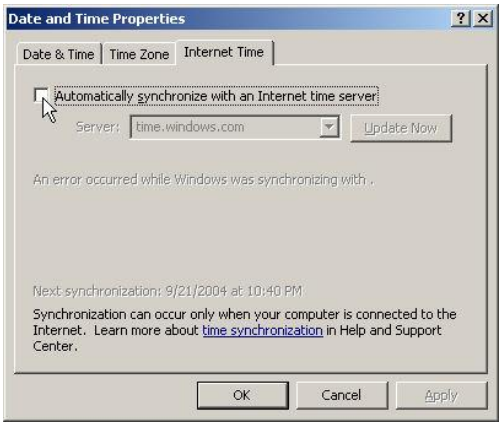


2. Make modifications as needed in the **Date & Time** tab interface.
3. To change the time zone, select the **Time Zone** tab and select a time zone from the drop-down menu.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



4. For the Evaluated Configuration, the time service must either be acquired from a Domain Controller or from the local system. On standalone computers, automatic time synchronization with external time servers must be disabled by deselecting the **Automatically synchronize with an Internet time server** check box in the **Internet Time** tab of the **Date and Time Properties** interface.



5. Computers that are members of a Windows Server 2003 domain will obtain their time from the Domain Controller and the **Internet Time** tab will be absent from the **Date and Time Properties** interface.

Note: If the time settings are modified on a computer that is not a domain member, the settings will take effect immediately. If the time settings on a domain client are modified locally, they will only be in effect until the time service synchronizes with the domain controller. When time synchronization with the domain time service occurs, the time on the domain client will be reset to match the time provided by the domain controller. Time synchronization within a domain may take several minute, which can vary depending on whether the client's current time settings are ahead or behind that of the domain controller.

Execute Diagnostic Tests – Error Checking Tool

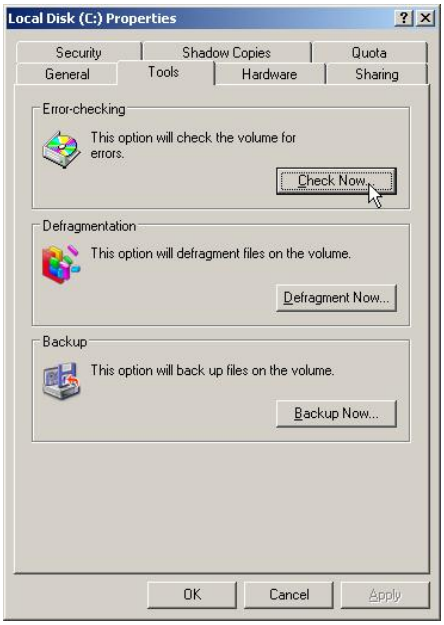
The error-checking tool can be used to check for file system errors and bad sectors on the hard disk.

Checking for file errors and bad sectors on a hard disk

1. Click **Start**, and select **My Computer**.
2. Right-click the disk volume that is to be checked, and then select **Properties**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

3. In the **Properties** interface, click the **Tools** tab.
4. Under **Error-checking**, click **Check Now**.



5. Under **Check disk options**, select the **Scan for and attempt recovery of bad sectors** check box.

Note: All files must be closed for this process to run. If the volume is currently in use, a message asks if the disk checking can be rescheduled for the next time the system is restarted. Then, the next time the system restarts, disk checking will run. The volume will not be available to run other tasks while this process is running. If the volume is formatted as NTFS, Windows Server 2003 automatically logs all file transactions, replaces bad clusters automatically, and stores copies of key information for all files on the NTFS volume.

Defining and Managing Security Templates

This subsection describes how to manage security templates in Windows Server 2003. A security template is a physical representation of a security configuration, and is a file where a group of security settings may be stored. Windows Server 2003 includes a set of security templates. The default settings in the templates cannot be used in the Evaluated Configuration. They can however, be modified to address Evaluated Configuration requirements as well as the Evaluated Configuration recommended settings as may be applicable to an implementing organization. Optionally, a set of security configuration templates is available with the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* for the Evaluated Configuration.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Starting Security Templates

1. Decide whether to add security templates to an existing console or create a new console:
   - To create a new console, click **Start**, select **Run**, type **mmc**, and then click **OK**.
   - To add security templates to an existing console, open the console.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Select **Security Templates**, click **Add**, click **Close**, and then click **OK**.
4. On the **Console** menu, click **Save**.
5. Type the name to be assigned to this console, and then click **Save**.

Note: By default, the saved console appears in the **My Documents** folder.

Customizing a Predefined Security Template

1. In the **MMC**, expand **Security Templates**.
2. Expand the default path folder (Systemroot\Security\Templates), and then right-click the predefined template that is to be modified.
3. Click **Save As**, and then type a file name for the security template.
4. Expand the new security template to display the security policies (such as **Account Policies**), and then double-click the security policy that to be modified.
5. Select the security area that is to be customized (such as **Password Policy**), and then double-click the security attribute to modify (such as **Minimum Password Length**).
6. Make the necessary modifications and click **OK**.

Defining a Security Template

1. In the **MMC**, expand **Security Templates**.
2. Right-click the template path folder where the new template will be stored, and then click **New Template**.
3. Type the name and description for the new security template. The new template then appears in the console tree.
4. Expand the new security template to display the security policies.
5. Expand the security policy (such as **Account Policies**) that is to be customized, and then click the security area (such as **Password Policy**).
6. Double-click the security attribute that is to be configured (such as **Minimum Password Length**).
7. Make the necessary modifications and click **OK**.

Deleting a Security Template

1. In the **MMC**, expand **Security Templates**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

2. Expand the template path folder where the security templates are stored, and then right-click the security template that is to be deleted.
3. Select **Delete**.

Refreshing the Security Template List

1. In the **MMC**, expand **Security Templates**.
2. Right-click the template path folder where the security templates are stored.
3. Select **Refresh**. The console tree displays any new additions or deletions.

Setting a Description for a Security Template

1. In the **MMC**, expand **Security Templates**.
2. Right-click **Security Templates**, the security template path folder, or a security template.
3. Click **Set Description**.

Applying a Security Template to a Local Computer

1. Click **Start**, select **Run**, type **mmc**, and then click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Select **Security Configuration and Analysis**, click **Add**, click **Close**, and then click **OK**.
4. In the **MMC**, right-click **Security Configuration and Analysis**.
5. If a working database is not already set, select **Open Database** to set a working database. Enter the name for the database and click **Open**.
6. Browse to locate the desired security template, select the template, and click **Open**.
7. Right-click **Security Configuration and Analysis**, and then click **Configure System Now**. Note that many of the security settings take effect immediately.
8. Reboot the computer.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Security-Relevant Events

This subsection describes all types of security-relevant events and what administrator action (if any) to take in order to maintain security. Security-relevant events that may occur during operation of Windows Server 2003 must be adequately defined to allow administrator intervention to maintain secure operation. Security-relevant events are defined as events that signify a security related change in the system or environment. These changes can be grouped as routine or abnormal. The routine events are already addressed in subsection Security Functions. For example a new person joins the organization, the administrator would setup a new account. Abnormal events are those that do not occur on regular basis or are a result of limits being reached as set by the Administrator. The security relevant events are based on the security functions defined in the Windows 2003/XP V3 ST.

Audit Trail Overflow

Description of Event: The audit log has reached its maximum capacity due to: 1) reaching the pre-defined maximum log size, or 2) running out of disk space.

Security Impact: Audit information cannot be recorded in the Security log. As a result, important audit information may be irretrievably lost.

Required Activities:

1. Archive the audit log.
2. Clear the audit log.
3. Re-examine the maximum log size requirements to ensure it is appropriate for current operations and make the necessary corrections.
4. Review audit requirements to ensure only relevant audit information is collected.
5. Review and make necessary adjustments to audit maintenance procedures to ensure the frequency of audit archives is sufficient to meet requirements without the need for system downtime or loss of audit data.
6. Depending on mission impact, consider setting the registry to halt the system when the audit log gets full. This will prevent further activities on the system without the benefit of being audited, however it can impact operations if audit maintenance is not followed on a regular basis.
7. Examine disk space requirements and make necessary adjustments by extending the disk volume, relocating the log file to a larger disk or partition, or replacing the disk drive with one of larger capacity.

Note: Procedures for archiving event logs are provided in the Archiving an Event Log subsection. Procedures for relocating an event log file are provided in the Change the default Event Viewer log location subsection.

Review Audit Trails for Suspected Malicious or Illicit Activity

Description of Event: Suspicion of malicious or illicit activity by either a known user or an unknown entity.

Security Impact: The risk implications depend on the type of activity that is under suspicion, keeping in mind that further investigations may reveal the underlying intent of the activity and either elevate or reduce the expected level of risk. Suspected activities could include; attempts to guess or brute force account passwords, unauthorized or suspicious object access attempts, unusual login hours, account activity while user is not expected to be logged in, unexpected modification of files or loss of data, etc.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Required Activities:

1. First, consult the Security Manager.
2. Once the suspect account has been identified, use the Event Viewer filtering tool in the Security Log Properties applet to filter through the logs for all event activities captured for that account.

   Note: Detailed instructions are provided in the Audit Management subsection (filtering the security log).

3. Disable the account, if warranted, based on Security Manager's recommendations.

   Note: Procedures for disabling the account are provided in the Disabling and enabling user accounts subsection.

4. Review the archived audit logs for any previous activity by the suspect account.
5. If suspect account is unknown, but data tampering is suspected, audit the group Everyone for access to all objects or types of objects suspected of being targets of tampering. Monitor the audit logs to determine if tampering is occurring and by whom.

   Note: Procedures and recommendations for auditing object access are provided in the Enabling Object Auditing subsection.

User Account is Disabled Due to Exceeded Limit of Unsuccessful Login Attempts

Description of Event: User account has been locked due to exceeding the established number of allowable failed login attempts.

Security Impact: Locked account impedes user from accomplishing required tasks. This incident could be the result of an attempt to guess the user account's password.

Required Activities:

1. Consult the account owner to verify whether the account lockout was due to his/her attempts to log in.
2. If the user has forgotten his/her password, set a new default password that must be changed as soon as the user logs in. Unlock the account to allow the user to log in.

   Note: Procedures for unlocking a user account are provided in the Configuring Account Lockout Policies subsection.

3. If the account lockout is verified to not have been the result of user (account owner) actions, it may be an indication of a possible compromise attempt. Do not unlock the account until the audit logs have been reviewed to determine if there is other suspicious activity that may be related. This includes previous attempts against the same account and failed login attempts against other user account during a common period of time. Make sure to check for any successive failed login attempts followed immediately by a login success to the same account. This could indicate a success on the part of the intruder to gain user access. Check the logon event record for the logon type to determine if the attempts were local, or network based and for possible clues as to the source (Domain name, machine name, etc.). Make sure to consult and follow direction from the Security Manager throughout this entire process. Unlock the account only after receiving Security Manager approval.

Temporary User Accounts are Required (such as for contractor support)

Description of Event: Accounts are needed for individuals requiring access to network resources on a temporary and limited basis. These individuals may be contractors, or simply personnel from another part

Copyright © 2008 Microsoft Corporation.

All rights reserved.

of the local organization who require temporary access to resources for which they are not normally authorized.

Security Impact: Potential for unauthorized access. If access requirements are not properly assessed and implemented temporary users may gain access to resources for which they are not authorized, or may continue to have access to resources beyond the required period of time.

Required Activities:

1. Consult resource owners to determine resource access requirements for temporary users.
2. Consult Security Manager to ensure temporary users have been properly cleared for access.
3. Create user groups for each type of temporary access required and assign the minimum privileges required for the temporary accounts to perform required tasks.

   Note: Procedures to create group accounts and assign the appropriate privileges are provided in the Creating and Maintaining User and Group Accounts and the Configuring User Rights subsections.

4. Set permissions on resources to be accessed by group members to allow only the minimum access requirements for the temporary accounts to perform required tasks. For example; they may only need read access to certain documents, not write or delete.

   Note: Procedures to set permissions on resources are provided in the Setting Access Controls on Files, Folders, Shares, and Other System Objects in Windows Server 2003 subsection.

5. Audit the activities of the temporary account groups.

   Note: Procedures to audit activities are provided in the Local Policies subsection (Configuring Audit Policies).

6. Create the temporary accounts. Set their initial password to expire on first logon, requiring the user to create a new password.

   Note: Procedures to create accounts and set password options are provided in the User Accounts subsection.

7. As determined by the data owners, management, and the Security Manager, set logon time restrictions on the temporary accounts.

   Note: Procedures are provided to set logon time restrictions in the Configuring Logon Hours subsection.

8. As determined by the data owners, management, and the Security Manager, set an expiration date on all temporary accounts that is adequate for the amount of time the accounts will be required.

   Note: Procedures are provided to set an expiration date on accounts in the "Set an Account Expiration Date" subsection.

Security-Relevant Service Pack or Hot Fix Updates are Available

Description of Event: The latest SP or update patch addressing security concerns is made available by Microsoft.

Security Impact: The security fixes may address serious issues that should be corrected immediately, depending on how a system is being used, where it sits on the network, and the applications that it supports. On the other hand, security fixes may have an adverse impact on the applications being used and should therefore be thoroughly evaluated before being applied within operational environments.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Required Activities:

1. Review the security update descriptions to first determine if they are relevant and essential to current operations.
2. If the security updates are considered essential to current operations security, establish a process for testing the updates prior to operational implementation. This can be accomplished by testing the updates within a staging area. The staging area should consist of an isolated lab environment with sufficient resources to effectively emulate the local systems. The intent is to identify and mitigate any incompatibility associated with a proposed security update and any business applications prior to its implementation, thus minimizing any risks to operations, services, users, or data within the operational network.
3. Once tested and verified, apply approved security updates to systems within the organization.

Note: Procedures for applying SPs and update patches are referenced in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*.

4. Record all system changes in configuration control records and update system build specifications to include implementation of security updates.

User Joins a Different Part of the Organization, Requiring Access Changes

Description of Event: A user joins a different element of the organization, requiring changes to account privileges, object access, group membership, and/or Domain membership.

Security Impact: Changes in a user's area of responsibility may require access changes. Otherwise, the user may retain access to resources outside his/her new realm of responsibility.

Required Activities:

1. Review the user's new access requirements with department managers and the Security Manager to establish network service and resource requirements.
2. If the user is joining a different network domain, remove the account from the current domain and create a new account in the new domain. This may involve different administrators.
3. If the change occurs within the same domain, remove the user from any group accounts the user no longer has a need for.
4. Assign the user to appropriate group accounts, providing access to necessary resources.
5. Remove unneeded privileges and assign any new required privilege sets. Typically, this is best accomplished through group memberships.
6. Set a new password for the user. Set it to require the user to change the password at the next logon. This will force the user to change the password to one of his/her own.

Note: Procedures for all of the above recommendations are provided in the Creating and Maintaining User and Group Accounts subsection.

User Leaves Organization

Description of Event: A user leaves the organization and no longer requires access to network resources.

Security Impact: Potential for unauthorized access. If access authorizations are not promptly and properly removed, the user account may continue have access to network resources beyond the time the employee leaves the organization.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Required Activities:

1. Verify that the user has not encrypted any essential files or directories. If so, make sure they can be decrypted before deleting the user account.

   Warning: If the administrator changes the password for a local user account, the user's access to any previously encrypted files will be lost. Make sure there is a DRA or that an alternate account also has access to the encrypted files before deleting the user account. See the Data Recovery subsection for information on setting up and using a DRA.

2. Review any resources that may have permissions set for only this user, and change permissions as appropriate.
3. Once verified by appropriate department managers and the Security Manager, delete the user account.

User Forgets Password

Description of Event: The user has forgotten his/her account password.

Security Impact: The user cannot log in and is unable to gain necessary resource access and perform required tasks.

Required Activities:

1. First verify that the user is authorized access. This is to ensure that the request is not a social engineering attempt.
2. Set a new password for the user. Set it to require the user to change the password at the next logon. This will force the user to change the password to one of his/her own.

   Note: Procedures to set password options are provided in the User Accounts subsection.

   Warning: If the administrator changes the password for a local user account, the user's access to any previously encrypted files will be lost. Make sure there is a DRA or that an alternate account also has access to the encrypted files before deleting the user account. See the Data Recovery subsection for information on setting up and using a DRA.

Recovery of User Encrypted Files

Description of Event: A user is unable to access his/her encrypted information, or leaves the organization without decrypting data required by the organization.

Security Impact: Valuable information could be inaccessible to the organization.

Required Activities:

1. If users are unable to decrypt previously encrypted data, or if an employee suddenly leaves the organization, a recovery agent - a user designated to recover encrypted files - can recover encrypted files on a computer using a recovery policy. Recovery policies are accessible through the Local Security Policy interface on standalone computers or are inherited from a Domain Security Policy. In Windows 2000 a default recovery policy is created for all standalone computers, and the local administrator is the recovery agent. In Windows Server 2003 and Windows XP Professional standalone computers there is no default recovery policy and, if desired, one must be created by an authorized administrator.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: Procedures for creating a DRA on a standalone Windows Server 2003 computer are provided in the Data Recovery on Stand-alone Windows Server 2003 subsection.

2. In order to recover encrypted files, the recovery agent must log onto the computer and decrypt the files.
3. If a user does not have access to the certificate and private key, he or she must rely on another recovery agent. Users back up the encrypted files using Backup or a similar backup utility. Then, they e-mail the backup files to a recovery agent, who then decrypts the files using the recovery agent's own recovery certificate and then e-mails the files back to the user. In a Windows Server 2003 domain, the domain administrator is the default recovery agent on all domain Windows XP and Windows Server 2003 clients. In order for a domain DRA to recover a user's encrypted files, they must be copied to a location where the DRA's private key can be used.
4. To protect the recovery certificate and its associated private key, recovery agents should remove the recovery certificate from the Certificate Manager after they export it to a backup file, as described in the previous subsection. Doing so prevents other people from gaining access to the recovery certificate and private key. Recovery agents can identify the certificate to be removed because the Certificate Manager describes its intended purpose as "File Recovery." After exporting the recovery certificate to a PFX file, they can remove it from the Certificate Manager; this ensures that the exported PFX file contains the only copy of the private key. They should put the PFX file in a safe place and import it into the Certificate Manager only when they must recover encrypted files on the computer.
5. In a Windows Server 2003 domain, the domain administrator creates recovery policies at the domain, the organizational unit, or the computer level. In this case, the default recovery agent is the domain administrator. Domain administrators should secure the recovery certificate and associated private key by exporting it and then deleting it from the Certificate Manager. The exported PFX file should then be stored in a safe place. Also, in a Windows Server 2003 domain, administrators can create additional recovery certificates and designate certain users as recovery agents.

Incorrect Time

Description of Event: The computer does not keep current time. This could be due to a number of issues, such as; the computer was moved to a location outside the original time zone; the system bios is not maintaining time; daylight savings time has taken effect and computer has not adjusted; the computer has acquired its time from a source that has the incorrect time.

Security Impact: Audit record on the affected system will not reflect the actual time that events took place.

Required Activities:

1. Check the BIOS battery to make sure it is charged. If it is not, replace the battery and set the proper time on the computer.
2. If the problem is due to a time zone change, set the correct time zone on the computer and reset the time to the proper time zone settings.
3. On the **Date/Time Properties** applet, click on the **Time Zone** tab and make sure the "**Automatically adjust clock for daylight saving changes**" box is checked.

Note: Procedures for accessing the **Date/Time Properties** applet are provided in the Set the Date and Time subsection.

4. Set the computer to get its time from a reliable timeserver.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: If the time settings are modified on a computer that is not a domain member, the settings will take effect immediately. If the time settings on a domain client are modified locally, they will only be in effect until the time service synchronizes with the domain controller. When time synchronization with the domain time service occurs, the time on the domain client will be reset to match the time provided by the domain controller. Time synchronization within a domain may take several minute, which can vary depending on whether the client's current time settings are ahead or behind that of the domain controller.

Quota Limit Reached

Description of Event: The administrator is alerted that a user's quota limit is being reached.

Security Impact: If the option of denying disk space to users who exceed their quota limit is selected, the user will receive an "out of disk space" message and will not be able to write additional data to disk. This result in a denial of service (storage) condition for the user by not allowing the user the ability to store work related information.

Required Activities:

1. Consult the user and review his/her disk space requirements.
2. Ask the user to delete unnecessary files, or move them to a back up location.
3. Alternatively, increase the user's disk quota if it is deemed appropriate.

Note: Procedures for all of the above recommendations are provided in the "Managing Disk Quotas" subsection.

It is Necessary to Revoke a User's Access to Objects and/or to the User's Privileges

Description of Event: It is necessary to immediately revoke a user's security attributes and revoke a user's access to objects.

Security Impact: It may be necessary to revoke access to certain objects and/or to remove certain privilege capability from a user due to changes in responsibilities and access requirements or due to concerns of misuse. Continued access may allow the user access to unauthorized data or may pose a risk to the data due to misuse. Additionally, the user may perform privileged actions for which he/she is no longer authorized or trusted.

Required Activities:

1. Review permissions on pertinent objects and remove or change the user's access permissions as appropriate.
2. Review the user's group memberships and remove the user from any group that provides privileges that are no longer required by the user.
3. Review the User Rights Assignment policy and make sure the user is not specifically granted the undesired privileges.
4. Force the user to re-authenticate to the network by having the user the user log off of the network.

Note: Simply ending a user's active session (as described in the Disconnecting a user or users from a share or active session subsection) will disconnect the user, however, the user will still retain the privileges he/she was granted when initially logged on and would be able to re-establish the session. To avoid this, it will be necessary to locally log the user off of from the computer.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Access to an ADFS-enabled Web Application Must be Revoked from a Current User

Description of Event: A user who had been previously authorized to access an ADFS-enabled application must be denied access to that application to avert a potential security risk; however, the user is currently authenticated and has an open session that is running the application, and his or her security token has not yet expired. Therefore, the user's current level of access is unauthorized and must be terminated.

Security Impact: The user will continue to have unauthorized access to the application until the Web browser is closed on the client computer or the user's security token expires at the end of the normal expiration period as configured in ADFS. (The default token life is 60 minutes.)

Required Activities: The only method of terminating user access to an ADFS-enabled application is to directly access the user's computer, close down the browser software, and delete the cached authentication cookie. If the administrator has access to the user's desktop or the processes running on the user's computer, the administrator can use whatever means at his or her disposal to terminate the online session or Web browser process and to clean out the cookies from the Web cache.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

4. External Security Measures

The security environment of the Evaluated Configuration of Windows Server 2003, as described in the Windows 2003/XP V3 ST, does not include any requirements for the environment. Therefore, the secure operation of Windows Server 2003 does not depend on any requirements being met by the environment. Assumptions with respect to the environment are described in Section 3.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

5. Acronyms

3DES	Triple-DES
ACL	Access Control List
ACE	Access Control Entry
AD	Active Directory
ADFS	Active Directory Federation Services
ADSI	Active Directory Service Interfaces
AES	Advanced Encryption Standard
AH	Authentication Header
API	Application Programming Interface
ASP	Active Server Pages
B2B	Business-to-Business
BIOS	Basic Input-Output System
CA	Certification Authority
CAL	Client Access License
CAPP	Controlled Access Protection Profile
CC	Common Criteria
CDP	Certificate Revocation List Distribution Point
CD-ROM	Compact Disk-Read Only Memory
CIFS	Common Internet File System
CIMC	Certificate Issuing and Management Components
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CN	Common Name
CPU	Central Processing Unit
CRL	Certificate Revocation List
CryptoAPI	Cryptographic API
CSP	Cryptographic Service Provider
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DC	Domain Controller
DCOM	Distributed Component Object Model
DDF	Data Decryption Field
DEP	Data Execution Prevention
DES	Data Encryption Standard

Copyright © 2008 Microsoft Corporation.
All rights reserved.

DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DN	Distinguished Name
DNS	Domain Naming System
DoS	Denial of Service
DPAPI	Data Protection API
DRA	Data Recovery Agent
DRF	Data Recovery Field
DTC	Distributed Transaction Coordinator
EFS	Encrypted File System
ESP	Encapsulating Security Protocol
EXE	Execute, Executable
FAT	File Allocation Table
FEK	File Encryption Key
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
FRS	File Replication Service
FSP	Federation Service Proxy
FTP	File Transfer Protocol
FQDN	Fully Qualified Domain Name
GB	GigaByte
GPO	Group Policy Object
GUI	Graphical User Interface
HSM	Hardware Security Module
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HTTP
ICF	Internet Connection Firewall
ICS	Internet Connection Sharing
ICMP	Internet Control Messaging Protocol
ID	Identification
IE	Internet Explorer
IIS	Internet Information Services
IKE	Internet Key Exchange
IP	Internet Protocol
IPP	Internet Printing Protocol

Copyright © 2008 Microsoft Corporation.
All rights reserved.

IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISAKMP	Internet Security Association and Key Management Protocol
ISAPI	Internet Server API
IT	Information Technology
KB	KiloByte
KB/sec	KB per Second
KCC	Knowledge Consistency Checker
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LGPO	Local Group Policy Objects
LPC	Local Procedure Call
LSA	Local Security Authority
LSDOU	Local, Site, Domain, OU
MB	Megabytes
Mbps	Megabits Per Second
MD5	Message Digest 5
MMC	Microsoft Management Console
NetBIOS	Network BIOS
NNTP	Network News Transfer Protocol
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTLMv2	New Technology LAN Manager Version 2
OCS	Operator Card Set
OID	Object Identifier
OS	Operating System
OU	Organizational Unit
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RIP	Routing Information Protocol
RFC	Request for Comment

Copyright © 2008 Microsoft Corporation.
All rights reserved.

RPC	Remote Procedure Call
RSA	Rivest, Shamir, and Adleman
RSoP	Resultant Set of Policy
RSVP	Resource Reservation Protocol
SA	Security Association
SACL	System Access Control List
SAM	Security Assurance Mechanism
SAML	Security Assertion Markup Language
SCSI	Small Computer System Interface
SCW	Security Configuration Wizard
SHA1	Secure Hash Algorithm 1
SID	Security Identifier
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Pack
SPN	Service Principal Name
SSI	Server Side Includes
SSL	Secure Sockets Layer
SSL/PCT	SSL/Personal Communication Technology
SSO	Single Sign-On
SMB	Server Message Block
S/MIME	Secure Multi-purpose Internet Mail Extensions
SNMP	Simple Network Management Protocol
SPN	Service Principal Name
SQL	Structured Query Language
SSP	Security Support Provider
ST	Security Target
SYSVOL	System Volume
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDO	Trusted Domain Objects
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol

Copyright © 2008 Microsoft Corporation.
All rights reserved.

UI	User Interface
UNC	Universal Naming Convention
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
WAN	Wide Area Network
WebDAV	Web Distributed Authoring and Versioning
WINS	Windows Internet Naming Service
WMI	Windows Management Instrumentation
XML	Extensible Markup Language
XrML	eXtensible Rights Markup Language

Copyright © 2008 Microsoft Corporation.
All rights reserved.

6. References

- A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003 |http://support.microsoft.com/kb/875352
- About WebDAV |http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/pub_dav_aboutwebdav.mspx
- Access control in Active Directory |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/security_accesscontrol.asp
- Active Directory Replication Model Technical Reference |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/a860fc4d-ca3c-4d03-b83b-74147dcfc0d9.mspx
- Availability of hardware-based Data Execution Prevention on multiprocessor systems that are running Windows Server 2003 with Service Pack 1 |http://support.microsoft.com/?kbid=902247
- Best Practices for Delegating Active Directory Administration |http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3&displaylang=en
- Certificate Autoenrollment in Windows Server 2003 |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/plan/autoenro.asp
- Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001.
- Certutil tasks for backing up and restoring certificates |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_cs_certutil8.asp
- Configuring Digest Authentication |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sec_auth_digestauth.asp
- Creating Publishing Directories (WebDav) |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/pub_dav_createpubdir.asp
- Encrypting and decrypting data |http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_seconceptsunencrypt.mspx
- Encryption |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sec_encryp_encryption.asp
- Group scope |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/sag_ADgroups_3groupscopes.asp

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- How To Add and Remove Web Service Extension Files in IIS 6.0 |http://support.microsoft.com/default.aspx?scid=kb;en-us;328419
- How to determine that hardware DEP is available and configured on your computer |http://support.microsoft.com/kb/912923
- How to relocate the SYSVOL tree on a domain controller that is running Windows 2000 Server or Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;842162
- HOW TO: Create a Secure WebDAV Publishing Directory |http://support.microsoft.com/default.aspx?scid=kb;en-us;323470
- HOW TO: List Web Server Extensions and Extension Files in IIS 6.0 |http://support.microsoft.com/default.aspx?scid=kb;EN-US;328505
- IIS Technical Reference: Securing Your Web Site with Web Permissions |http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_TAS_28.mspx
- Integration Guide: Microsoft Certificate Services and nCipher Modules (Configuring an nCipher Module with Windows Server 2003), September 30, 2003.
- Internet Information Services (IIS) FAQ |http://www.microsoft.com/windowsserver2003/community/centers/iis/iis_faq.mspx
- Internet Information Services 6.0 Product Documentation |http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/iiswelcome.mspx
- Introducing the Windows Server 2003 Family |http://www.microsoft.com/windowsserver2003/evaluation/overview/family.mspx
- Key Archival and Management in Windows Server 2003 |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/kyacws03.asp
- Managing WebDAV Security |http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/pub_dav_webdavsecurity.mspx
- Microsoft Knowledge Base Article 322692: How to raise domain and forest functional levels in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;322692
- Microsoft Knowledge Base Article 323276: How To Install and Use RSoP in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;323276
- Microsoft Knowledge Base Article 323428: HOW TO: Configure Internet Printing in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;323428
- Microsoft Knowledge Base Article 323470: HOW TO: Create a Secure WebDAV Publishing Directory |http://support.microsoft.com/default.aspx?scid=kb;en-us;323470
- Microsoft Knowledge Base Article 324274: How To Configure IIS Web Site Authentication in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;324274
- Microsoft Knowledge Base Article 324276: HOW TO: Configure Internet Information Services Web Authentication in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;324276
- Microsoft Knowledge Base Article 326020: How to configure IIS 6.0 URL Authorization |http://support.microsoft.com/default.aspx?scid=kb;en-us;326020#1

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Microsoft Knowledge Base Article 328419: How To Add and Remove Web Service Extension Files in IIS 6.0 |http://support.microsoft.com/default.aspx?scid=kb;en-us;328419
- Microsoft Knowledge Base Article 328505: HOW TO: List Web Server Extensions and Extension Files in IIS 6.0 |http://support.microsoft.com/kb/328505/EN-US/
- Microsoft Knowledge Base Article 810207: IPSec Default Exemptions Are Removed in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;810207
- Microsoft Knowledge Base Article 812614: Default permissions and user rights for IIS 6.0 |http://support.microsoft.com/?scid=kb;en-us;812614&spid=2097&sid=global
- Microsoft Knowledge Base Article 816117: HOW TO: Configure Web Permissions for Web Content in Internet Information Services 6.0 |http://support.microsoft.com/default.aspx?scid=kb;en-us;816117
- Microsoft Knowledge Base Article 816514: HOW TO: Configure IPSec Tunneling in Windows Server 2003 |http://support.microsoft.com/default.aspx?scid=kb;en-us;816514
- Microsoft TechNet - Checklist: Creating a certification hierarchy with an offline root certification authority |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/45c28bf8-9952-4ca1-b124-7d86afb83f69.mspx
- Microsoft TechNet - Configure an offline root certification authority to support certificate revocation with Active Directory |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/4722dc0f-ca69-446a-a7b0-35886b278d72.mspx
- Microsoft TechNet: Active Directory Federation Services (ADFS http://technet2.microsoft.com/WindowsServer/en/Library/050392bc-c8f5-48b3-b30e-bf310399ff5d1033.mspx
- Microsoft TechNet: ADFS Concepts http://technet2.microsoft.com/WindowsServer/en/Library/4147976b-8518-4ae0-804b-8723645f04ae1033.mspx
- Microsoft TechNet: ADFS How To http://technet2.microsoft.com/WindowsServer/en/Library/d022ac37-9b74-4ba1-95aa-55868c0ebd8c1033.mspx
- Microsoft TechNet: ADFS Operations Guide http://technet2.microsoft.com/WindowsServer/en/Library/ed76b687-7585-421d-ad41-47c21499de001033.mspx
- Microsoft TechNet: Administer a Certification Authority |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/4af2007c-a5be-4fae-86d1-311dd986e4e5.mspx
- Microsoft TechNet: Administering Active Directory Federation Services http://technet2.microsoft.com/WindowsServer/en/Library/007d4d62-2e2e-43a9-8652-9108733cbb731033.mspx
- Microsoft TechNet: Best Practices for Implementing a Microsoft Windows Server 2003 Public Key Infrastructure |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws3pkibp.mspx#EZAA
- Microsoft TechNet: CA Certificates Tools and Settings |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/d5c1c4dd-7ee8-4df8-a3b0-5ae40a34e45b.mspx

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Microsoft TechNet: Configure Replication Between Sites |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/49ffcb72-b471-4a0a-a889-f9ecd0b099f3.mspx
- Microsoft TechNet: Deploying and Configuring Internet Information Services (IIS) 6.0 with Remotely Stored Content on UNC Servers and NAS Devices |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/webapp/iis/remstorg.mspx
- Microsoft TechNet: How Active Directory Functional Levels Work |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/c3aa5e55-42c0-4386-93ba-66e5c538b0ac.mspx
- Microsoft TechNet: Installing and configuring a certification authority |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_CS_Setup.asp
- Microsoft TechNet: Selecting Certificate Enrollment Options |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/aacff17c-acee-4017-9ddc-957ff2e4eedc.mspx
- Microsoft TechNet: Smart Cards |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/bcac4007-45cf-4260-876c-7bfca5a01a8a.mspx
- Microsoft TechNet: Troubleshooting Active Directory Federation Services http://technet2.microsoft.com/WindowsServer/en/Library/1eb6840d-3e5e-42d1-b310-41772a8a095a1033.mspx
- Microsoft TechNet: Understanding Active Directory |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/1c000ff6-3c18-4ef2-9f61-cac960be4889.mspx
- Microsoft TechNet: Using role separation |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_cs_usingroleseparation.asp
- Microsoft TechNet: What Are Domain and Forest Trusts? |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/TechRef/3215e730-c1a7-4918-bc9e-67f343f89e61.mspx
- Microsoft TechNet: Windows Server 2003 Security, Chapter 10: Hardening Certificate Services Servers |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/win2003/w2003hg/sgch10.asp
- Microsoft Windows Server 2003 TechCenter |http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/2e0186ba-1a09-42b5-81c8-3ecca4ddde5e.mspx
- Microsoft Windows Server 2003 TechCenter: Windows Server 2003 Internet Information Services (IIS) |http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_TAS_28.mspx
- MSDN Home: How To Use IPSec |http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod111.asp
- nCipher's Hardware Installation Guide, April 19, 2005.
- nCipher's nShield/payShield User Guide Windows, June 18, 2003.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Physical Address Extension - PAE Memory and Windows |http://www.microsoft.com/whdc/system/platform/server/PAE/PAEdrv.mspx
- PKCS #10 (Certification Request Syntax Standard).
- Public Key Cryptography Standard (PKCS) #7 (Cryptographic Message Syntax Standard).
- Remote EFS Operations in a Web Folder Environment |http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prnb_efs_xqao.asp
- Remote EFS Operations on File Shares and Web Folders |http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prnb_efs_hzqx.asp
- RFC 2797 CMC (Certificate Management Messages over Cryptographic Message Syntax).
- RFC 3280 Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
- RSoP overview |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/RSPoverview.asp
- Securing Sites with Web Site Permissions |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sec_acc_settwebperm.asp
- Securing WebDAV Publishing Directories |http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_SEC_29.mspx
- Smart Cards |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_SC_topnode.asp
- Step-by-Step Guide to Administering Certificate Services |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/howto/admncert.asp
- Step-by-Step Guide to Internet Protocol Security (IPSec) |http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp
- Tech Net. HOW TO: Back Up and Restore a Certification Authority in Windows 2000 |http://support.microsoft.com/default.aspx?scid=kb;en-us;313272&sd=tech
- To request a certificate |http://www.microsoft.com/windows2000/en/server/help/sag_CMprocsReqCert.htm
- Understanding Group Policies on Windows Server 2003 |http://www.microsoft.com/technet/community/events/windows2003srv/tnt1-86.mspx
- Using Microsoft Windows IPSec to Help Secure an Internal Corporate Network Server |http://www.microsoft.com/downloads/details.aspx?FamilyID=a774012a-ac25-4a1d-8851-b7a09e3f1dc9&displaylang=en

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Using the Active Directory Installation Wizard |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_adPromoteDCs.asp
- Using Virtual Directories |http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/qss_wss_virtdirectories.mspx
- Web Authoring with WebDAV |http://www.microsoft.com/resources/documentation/iis/6/all/proddocs/en-us/pub_dav_webdav.mspx
- WebDAV Publishing Directories |http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_CFG_6.mspx
- WebDAV Redirector |http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/pub_dav_redirector.asp
- What Is the Active Directory Replication Model? |http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/all/techref/en-us/w2k3tr_repup_what.asp
- Windows Cannot Find a Certification Authority That Processes the Request |http://support.microsoft.com/default.aspx?scid=kb;en-us;271861
- Windows Server 2003 Deployment Kit. Chapter 16: Designing a Public Key Infrastructure. |http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx
- Windows Server 2003 PKI Operations Guide |http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/ws03pkog.asp
- Windows Server 2003 Technical Reference |http://www.microsoft.com/Resources/Documentation/windowsserv/2003/all/techref/en-us/?frame=true
- Windows XP Resource Kit |http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prnb_efs_xqao.asp
- Windows XP Resource Kit, Chapter 17, Encrypting File System |http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prnb_efs_hzqx.asp

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Appendix A – Windows Server 2003 Certificate Server Security Configuration Guide

This Appendix provides procedures for the installation and configuration of Windows Server 2003 Certificate Server on the Evaluated Configuration of Windows Server 2003, Enterprise Edition. Within this appendix, TOE references pertain to the Windows Server 2003/XP Professional Evaluated Configuration, Version 3.0 TOE.

General Hardware and Operating Environment Configuration

The Windows Server 2003 Certificate Server is an optional service component of the Windows Server 2003 operating system. Prior to installing and configuring the Certificate Server, the host Windows Server 2003, Enterprise Edition with SP2 (32-bit version) operating system and supporting hardware environment should be configured in accordance to the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0*. This ensures that the host operating system itself has been securely configured to meet Common Criteria requirements.

Software Configuration

Within the Windows Server 2003 Evaluated Configuration, the configuration of a Certification Authority (CA) includes the Microsoft Windows Server 2003 Enterprise Edition running the Certificate Services component configured in any one of the roles shown in Table A-1 in accordance with the installation instructions provided in this document.

Table A-1 Certificate Server Roles for the Evaluated Configuration

Product	Role
Certificate Server component installed on the Microsoft Windows Server 2003, Enterprise Edition, with SP2 (32-bit version)	Enterprise Root CA Enterprise Subordinate CA

CA roles available in Microsoft Windows Server 2003 Enterprise Edition

Within the Windows Server 2003 Evaluated Configuration, a CA must only be configured as an Issuing CA and must be configured to use Active Directory. Offline CAs, stand-alone CAs, and any enterprise root CAs that do not issue certificates are not included in the Target of Evaluation (TOE) for Windows Server 2003, but may be considered as part of the supporting Public Key Infrastructure (PKI) environment.

Stand-alone CA roles are not options in the TOE for Windows Server 2003. Although a stand-alone CA can use Active Directory to publish certificates and revocation lists and can be configured to issue certificates automatically, it does not use Active Directory to validate certificates and does not interact with Active Directory to authenticate certificate requests. Additionally, it does not support the management of certificate templates.

- **Enterprise Root Certification Authority (CA):** An enterprise root CA is a top-level CA in a certification hierarchy. An enterprise root CA requires the Active Directory service. It self-signs its own CA certificate and uses Group Policy to publish that certificate to the Trusted Root Certification Authorities store of all servers and workstations in the domain. Normally, an enterprise root CA does not directly provide resources for user and computer certificates, but is the foundation for a certificate hierarchy. When configured in the Evaluated Configuration, the Enterprise Root CA must also be the issuing CA.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Enterprise Subordinate CA:** An enterprise subordinate CA must obtain its CA certificate from another CA. An enterprise subordinate CA requires Active Directory. Enterprise subordinate CAs are used to take advantage of Active Directory, certificate templates, and smart card logon to Windows XP and computers running Windows Server 2003 family operating systems.
- **Stand-alone Root CA:** A stand-alone root CA is a top-level CA in a certification hierarchy. The stand-alone root CA may or may not be a member of a domain and, therefore, does not require Active Directory. However, it will use Active Directory if it exists for publishing certificates and certificate revocation lists. Since a stand-alone root CA does not require Active Directory, it can easily be disconnected from the network and placed in a secure area, which is useful when creating a secure offline root CA. Although not included in the TOE for Windows Server 2003, a stand-alone root CA may be used as part of the PKI environment that supports the TOE.
- **Stand-alone Subordinate CA:** A stand-alone subordinate CA must obtain its CA certificate from another CA. The stand-alone subordinate CA may or may not be a member of a domain and, therefore, does not require Active Directory. However, it will use Active Directory if it exists for publishing certificates and certificate revocation lists. It must obtain its CA certificate from another CA. Although not included in the TOE for Windows Server 2003, a stand-alone subordinate CA may be used as part of the PKI environment that supports the TOE.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Certificate Server Installation

This section provides the installation procedures for the Windows Server 2003 Certificate Server.

Preparing for Installation

Prior to initiating the installation of a certificate server, there must be a clear understanding of the desired PKI architecture in order to define the types of CA roles that will be needed. In addition, during installation of the Certificate Server, the Setup program will ask for configuration information needed to proceed with the installation. Prepare for the Windows Server 2003 Certificate Server installation by preparing the hardware and operating environment and establishing configuration decisions prior to initiating the installation process. The following checklist provides some guidelines as to the information that needs to be defined prior to initiating the installation process.

Table A-2 Windows Server 2003 Certificate Server Pre-Installation Checklist

	Description
❑	**Operating Environment:** Ensure that the Windows Server 2003 Enterprise Edition operating system version is used as the host for the Certificate Server. The operating system should be configured in its Common Criteria Evaluated Configuration as defined in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0.*
❑	**CA Management Role Designations:** Administration of the Certificate Server will be controlled based on a set of CA management roles. Make sure authorized user accounts have been pre-defined for individual assignment to the CA Administrator, Officer, Auditor, and Backup Operator roles. Each designated user account must not be assigned to more than one CA management role.
❑	**PKI Architecture and Certificate Server Role:** Prior to initiating the installation of the Certificate Server, define the PKI infrastructure that will be supported and the CA role that will be applicable to the Certificate Server being installed. For information on defining a PKI infrastructure and supporting CA requirements the following references are recommended for review: ▪ Designing a Public Key Infrastructure http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b.mspx ▪ Planning a Microsoft Windows Public Key Infrastructure Using Microsoft Windows Server 2003 (an online presentation) http://www.microsoft.com/seminar/shared/asp/view.asp?url=/seminar/en/20030424vcon43/manifest.xml ▪ Build Guide - Implementing the Public Key Infrastructure http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/BGCH07.mspx ▪ Public Key Infrastructure for Windows Server 2003 http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx
❑	**Hardware Security Module (HSM):** Installation of the Windows Server 2003 Certificate Server in the Evaluated Configuration of Windows Server 2003, Enterprise Edition requires the use of an nCipher HSM. Ensure that all necessary hardware and software components are installed or available for the installation of the HSM prior to initiating the installation of the Certificate Server.
❑	**CA Naming Conventions:** Define the CA name (common name) and the naming convention that will be used within the PKI environment. For details on name constraints see http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/3c1f3475-9762-4c91-9a4c-dff76053d768.mspx.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

	Description
❑	**Network Membership:** Before installing a Certification Authority, configure the computer's Domain settings first, such as joining a domain or promoting a server to a domain controller. These settings cannot be changed once the certification authority is installed.
❑	**Active Directory Rights:** The enterprise root CA selection requires that the host computer be a member of a domain and that it use the Active Directory service. The administrator who is installing an enterprise CA must have Write permission to Active Directory. If the administrator installing the CA has Write permission to Active Directory, then specifying the shared folder is optional, and is not typically done for enterprise certification authorities.
❑	**Installation Media:** During the installation of the Windows Server 2003 Certificate Server, the operating system installation media will be searched for necessary installation files. Make sure the installation CD-ROM for the Windows Server 2003 Enterprise Edition operating system is available.
❑	**Service Components:** The computer hosting the Certificate Server should not host other services. Therefore, to reduce potential risks and improve system performance, it is recommended that any unnecessary services be disabled.

Windows Server 2003 Certificate Server Installation Process

Installation of the Hardware Security Module

The Windows Server 2003 Certificate Server hosted on the Windows Server 2003 Evaluated COnfiguration requires the use of the nCipher nShield HSM, hereafter referred to as the nCipher HSM. The nCipher HSM is a hardware encryption device that is connected to the Certificate Server at the device level via Peripheral Component Interconnect (PCI) or Small Computer System Interface (SCSI) interfaces. From an operating system view, the HSM interfaces through the Microsoft CryptoAPI interfaces at the logical level.

The Microsoft Windows Server 2003 Certificate Server provides several software based Cryptographic Service Providers (CSPs) that generate private keys which are archived and encrypted in a local protected store. The nCipher HSM is a hardware based CSP, which uses a tamper resistant, physically hardened enclosure to provide a higher level of protection for a Certificate Authority's private key. The nCipher HSM is compliant with both Federal Information Processing Standard (FIPS) 140-2 level 2 and level 3. Additional information on the nCipher NIST (National Institute of Standards and Technology) approved evaluations is available at http://csrc.nist.gov/cryptval/140-1/1401vend.htm. The following hardware model and firmware/software versions were used in the Evaluated Configuration.

- **HSM Model:** nShield F3 UltraSighn PCI – nC4032P-300
- **HSM Firmware Version:** 2.18.15
- **nCipher Support Software Version:** 10.15 for Windows

HSM Installation Procedures

The nCipher HSM must be installed properly prior to installing Certificate Services on the Windows Server 2003 computer that will be hosting the Certificate Server. Use the procedures described below to install the software and hardware components of the HSM.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Install the nCipher HSM

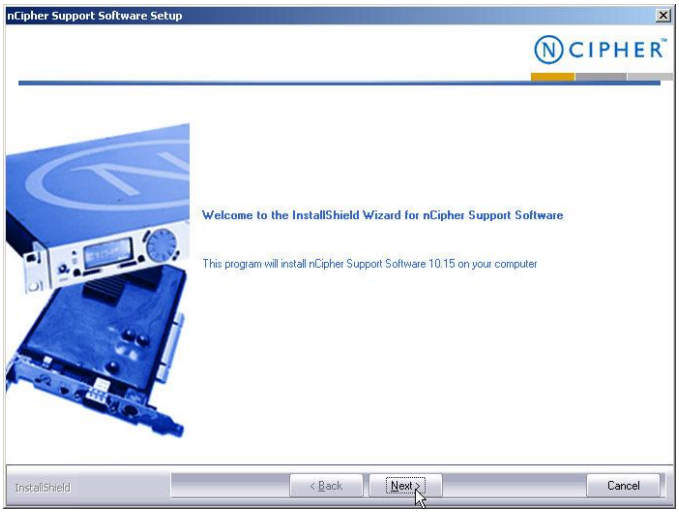
Refer to the nCipher Hardware Installation Guide for full instructions on installing the HSM. The nCipher hardware must be installed prior to initiating installation of the supporting software.

> **Note:** Prior to initiating the software installation, ensure that the two switches on the boars are set to the "off" position and the Mode switch on the exterior face of the HSM is set to "O." See the nCipher Hardware Installation Guide for details.

Install the nCipher Software

Install the nCipher software by performing the following tasks.

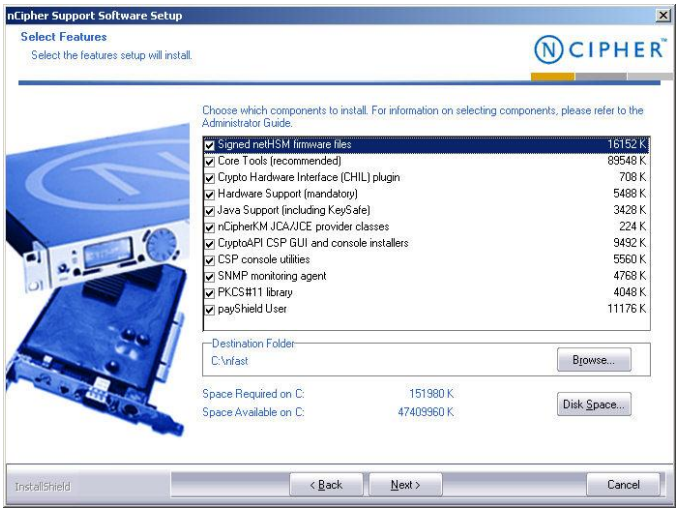
1. Log onto the Windows Server 2003 computer as local Administrator or as a user with local Administrator privileges.
2. Insert the nCipher CD that supports Windows Server 2003. The nCipher Support Software Setup program will automatically start. If it does not automatically start open Windows Explorer and navigate to the CD-ROM location and execute the installer manually by executing the **Setup.exe** program located at the root of the CD-ROM.
3. At the Welcome panel, click **Next**.



4. Accept the software license agreement by clicking **Yes**. The **Select Features** window will appear.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



- The default installation folder for all files is C:\nfast. An alternative installation folder may be selected.
- In the components selection box, select the components to be installed by checking or unchecking the selection box next to each component. The following list of components must be unchecked in the components selection box:
  - Java Support (including KeySafe)
  - nCipher KM JCA/JCE provider classes
  - SNMP monitoring agent

5. Click **Next**. The **Setup Status** window will appear as the installer performs the configuration of the selected components.

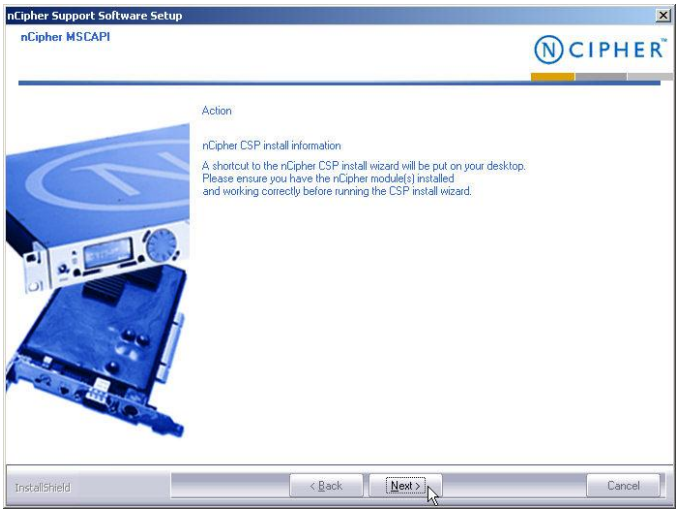
Note: A warning message may appear stating that the Sun Java Runtime Environment is needed for the KeySafe application to function properly. This has no impact on the configuration. Click **OK** on the warning message.

6. After the initial setup completes, an **nCipher MSCAPI** window will appear stating that it will create an icon on the desktop for the nCipher CSP install wizard. Click **Next**.

Warning: Do not run the shortcut until the hardware cryptographic module is configured for use.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



7. The **nCipher PKSC#11** selection window will appear. Select the **Yes** radio button to enable the Security Assurance Mechanism and click **Next**.

8. A message will appear asking if the PKCS#11 library should be configured for use with CheckPoint VPN-1/Firewall-1. Select the **No** radio button and click **Next**.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

9. The **InstallShield Wizard Complete** window will appear. Click **Finish**.
10. To verify that the software is installed correctly, click **Start** and select **Run**, type **cmd.exe**, and click **OK** to open a command line interface. From the command prompt, execute the following program:

    C:\nfast\bin\enquiry
11. Observe that the server and module modes are operational as shown in the example below.

```
Command Prompt

C:\Documents and Settings\Administrator>C:\nfast\bin\enquiry
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        A6AE-E4A4-D50C
 mode                 operational
 version              2.23.6
 speed index          294
 rec. queue           430..630
 level one flags      Hardware HasTokens
 version string       2.23.6cam6, 2.18.15cam1 built on Jun 01 2005 13:23:57
 checked in           0000000043 1dca98 Tue Sep 06 12:58:00 2005
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds
 module type code     0
 product name         nFast server
 device name
 EnquirySix version   4
 impath kx groups
 feature ctrl flags   none
 features enabled     none
 version serial       0
 remote server port   9004

Module #1:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        A6AE-E4A4-D50C
 mode                 operational
 version              2.18.15
 speed index          294
 rec. queue           15..152
 level one flags      Hardware HasTokens
 version string       2.18.15cam1 built on Jun 01 2005 13:23:57
 checked in           0000000042 80988f Tue May 10 07:18:39 2005
 level two flags      none
 max. write size      8192
 level three flags    KeyStorage
 level four flags     OrderlyClearUnit HasRTC HasNVRAM HasNSOPermsCmd ServerHasP
ollCmds FastPollSlotList HasSEE HasKLF HasShareACL HasFeatureEnable HasFileOp Ha
sLongJobs ServerHasLongJobs AESModuleKeys NTokenCmds
 module type code     6
 product name         nC1002P/nC3022P
 device name          #1 PCI bus 3 slot 5
 EnquirySix version   5
 impath kx groups     DHPrime1024
 feature ctrl flags   LongTerm
 features enabled     StandardKM
 version serial       24
 kneti hash           b3ffb394a50b8bc5d7cae51f6b84fd2352ba2e14
 rec. LongJobs queue  4
 SEE machine type     gen1AIF
```

12. Shut down the computer.
13. Once the computer has been shut down, reset the HSM to a pre-initialization state to enable the creation of a new security world and Administrator Cards.

Note: Set the Mode switch to "I." There is a switch on the exterior face of the HSM card. See the nCipher Hardware Installation Guide for details.

Create the nCipher Security World

The nCipher Security World permits the management of key life cycles. The security world is installed using the **nCipher CSP install wizard**. The wizard is used to:

- Create a new security world,
- Add a module to an existing security world,
- Create an Administrator Card Set,

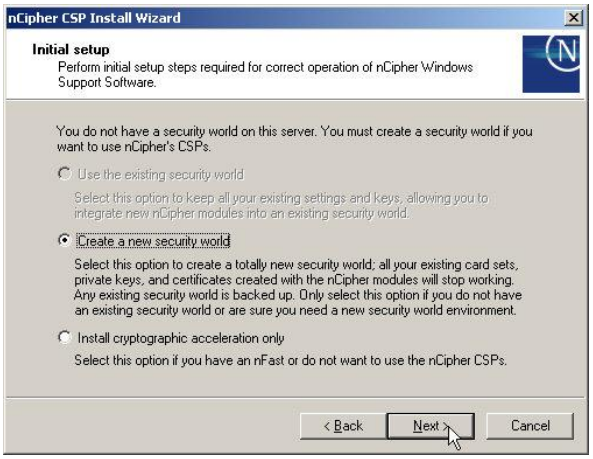
Copyright © 2008 Microsoft Corporation.

All rights reserved.

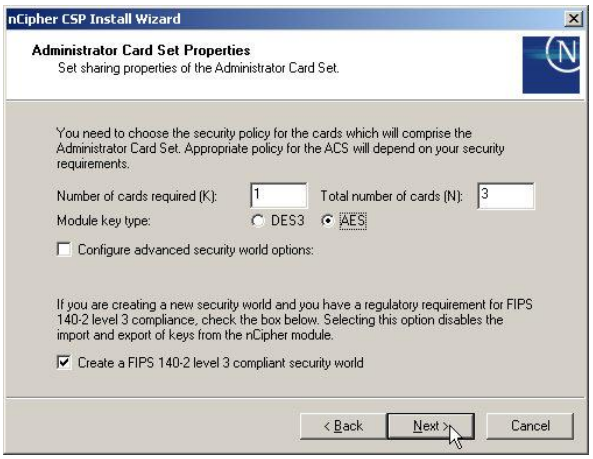
- Create an Operator Card Set, including K of N sets, and
- Install nCipher's Crypto API Cryptographic Service Provider or modexp offload.

Create an Administrator Card Set (ACS):

1. After the computer has been rebooted with HSM in pre-init mode, log onto the Windows Server 2003 computer as local Administrator or as a user with local Administrator privileges.
2. Start the CSP wizard by double clicking on the **nCipher CSP install wizard** icon on the desktop. When the **nCipher CSP Install Wizard** appears, click **Next**.
3. At the **Initial setup** view of the install wizard, select the radio button: **Create new security world**. Click **Next**.



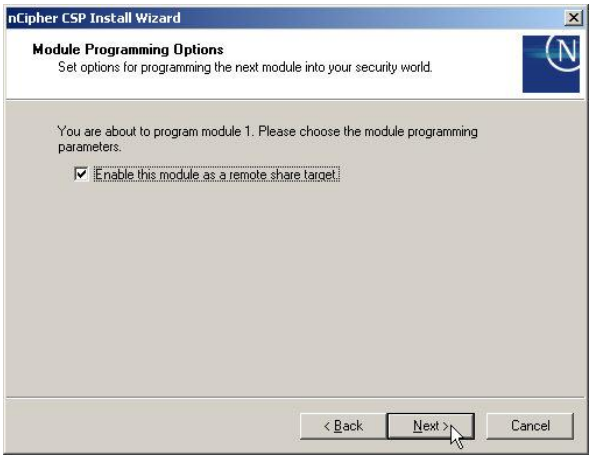
4. At the **Administrator Card Set Properties** view of the install wizard, select a security policy for the number of cards required (K) and the number of cards in the set (N) (recommendation: K = 1, N = 3). Choose either DES3 or AES for the Module key type, and check the box next to Create a **FIPS 140-2 level 3 compliant security world**. Click **Next**.



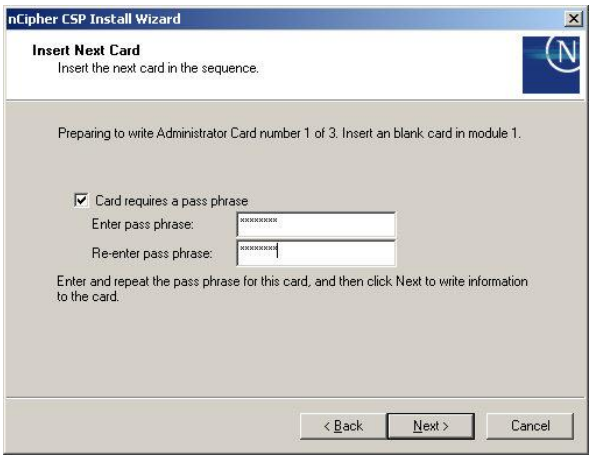
5. At the **Module Programming Options** view of the install wizard, accept the defaults (**Enable this module as a remote share target**) and click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



6. If an Administrator Card has not been inserted into card reader the **Next** button of the **Insert Next Card** view of the install wizard will be grayed out. Insert the first of three cards. The software will detect the card and the install wizard view will present an option for requiring a card pass phrase. Check the box next to **Card requires a pass phrase**. Enter and re-enter a pass phrase and click the **Next** button.



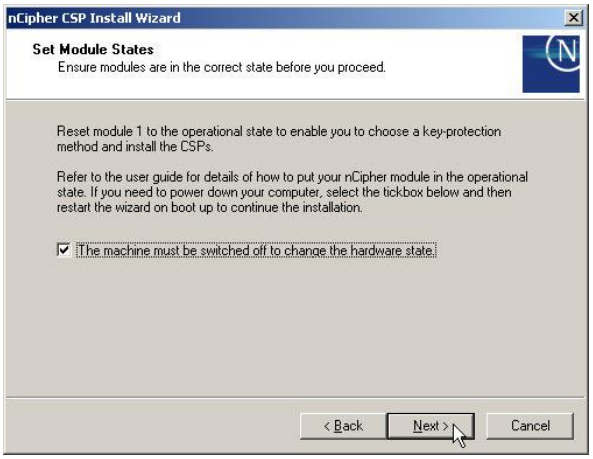
7. The wizard will request that the second Administrator Card be inserted. Insert the second Administrator Card. The software will detect the card and the install wizard view will present an option for requiring a card pass phrase. Check the box next to **Card requires a pass phrase**. Enter and re-enter a pass phrase and click the **Next** button.

8. The wizard will request that the third Administrator Card be inserted. Insert the third Administrator Card. The software will detect the card and the install wizard view will present an option for requiring a card pass phrase. Check the box next to **Card requires a pass phrase**. Enter and re-enter a pass phrase and click the **Next** button.

9. At the **Set Module States** view of the install wizard, remove the Administrator Card from the card reader and check the box next to **The machine must be switched off to change the hardware state**. Click the **Next** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

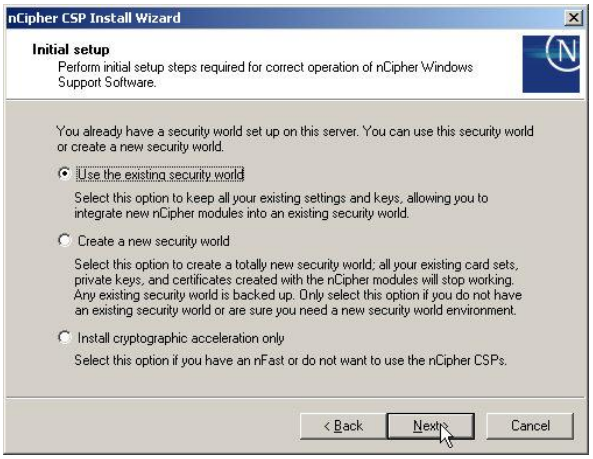


10. The wizard will state that a reboot is required. Click the **Finish** button and shut down the computer.
11. With the computer shut down, set the Mode switch on the HSM to "O," for Operational, and start the computer. The cryptographic module is now in the operational mode.
12. Restart the computer and log on as local Administrator or as a user with local Administrator privileges.
13. Check that the installation was successful by opening a command prompt and running the following program:

    C:\nfast\bin\enquiry
14. Observe that the server and module modes are operational.
15. Remain logged on to create the Operator Cards.

Create the Operator Card Set (OCS):

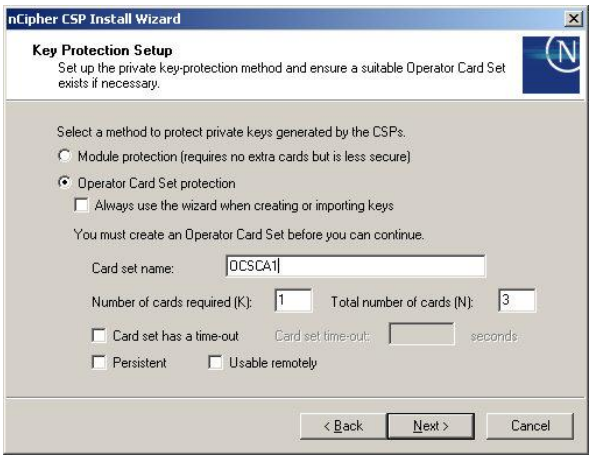
1. Insert an Administrator Card in the card reader.
2. Run the **nCipher CSP Install Wizard** again by double-clicking its shortcut on the Desktop.
3. T**he nCipher CSP Install Wizard** appears. Click **Next**.
4. A security world setup panel appears. It indicates that it detected the existing security world created earlier. Select the radio button electing to **Use the existing security world** and click **Next**.



Copyright © 2008 Microsoft Corporation.

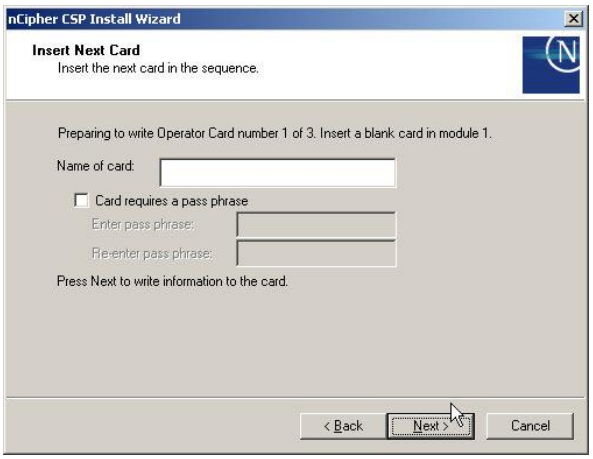
All rights reserved.

5. A **Key Protection Setup** window appears prompting for the method of key protection, module key or OCS, and the K of N quorum. Other options to decide are: persistent; time out; and remote usage. Fill in the answers on this panel as follows:



- Select the **Operator Card Set protection** radio button to create an operator card set.
- Name the card set. (for example, OCSCA1)
- Number of Cards required: 1
- Total number of cards: 3
- Set a card time-out, if desired
- Do not select the option to create persistent cards.
- Click **Next**

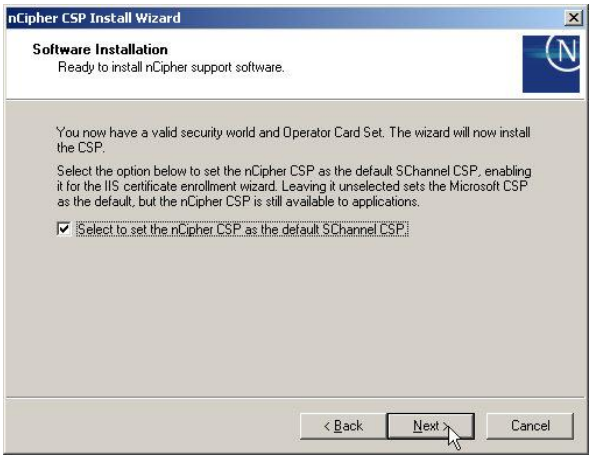
6. An **Insert Next Card** panel appears for each card. Remove the Administrator Card and insert the first card for the OCS. If a passphrase for using the card is not desired, do not check the **Card requires a passphrase** box. Name the card, if desired. Click **Next**. Repeat this procedure for the next two cards.



7. A **Software Installation** panel will appear indicating that there is a valid security world and operator card set. Check the box next to **Select to set the nCipher CSP as the default SChannel CSP**. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



8. The install wizard will indicate that the nCipher CSPs have been installed and the security world is ready for use. Click **Finish**.

Installation of the Windows Server 2003 Certificate Server

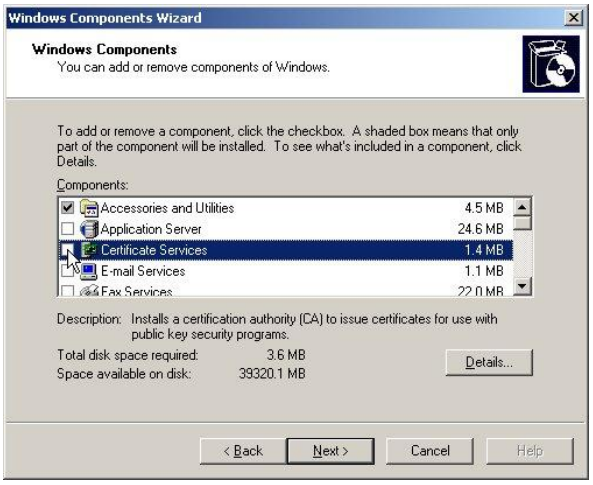
Use the following steps to install the Windows Server 2003 Certificate Server using the installed nCipher hardware-based CSP.

Windows Server 2003 Certificate Server Installation

1. To install an Enterprise root CA or an Enterprise subordinate CA, log on as a member of both the Enterprise Admins group and the root domain's Domain Admins group.

   Note: Stand-alone CAs are not in the TOE for Windows Server 2003, but may be used as part of the supporting PKI environment.

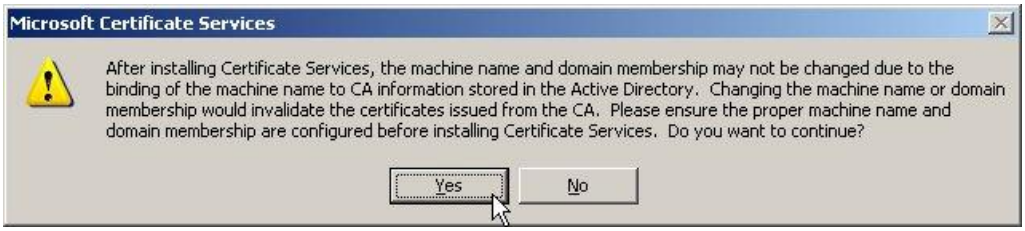
2. Click the **Start** button, point to **Control Panel**, and select **Add or Remove Programs**.
3. When the **Add or Remove Programs** dialog box appears, click **Add/Remove Windows Components**. A **Windows Components Wizard** dialog box will appear.



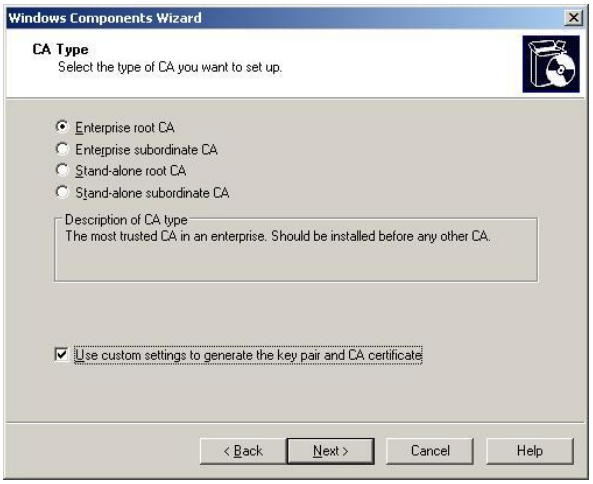
Copyright © 2008 Microsoft Corporation.

All rights reserved.

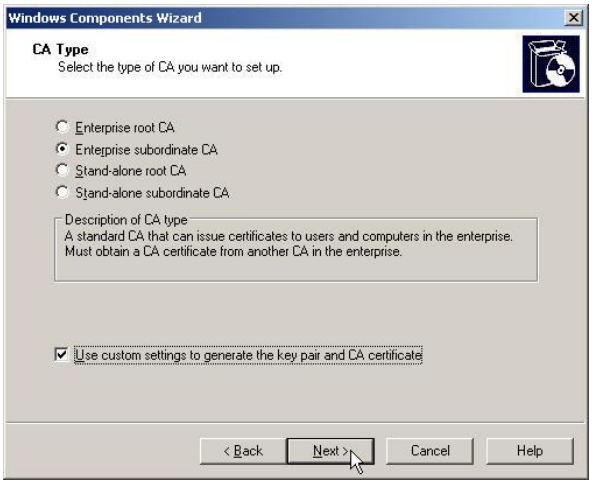
4. In the **Components** window of the **Windows Components Wizard** dialog box, click the check box next to **Certificate Services**. A warning message will appear as shown below. Click **Yes** to continue. Then click **Next** on the **Windows Components Wizard**.



5. When the **CA Type** dialog box of the **Windows Components Wizard** is displayed, select the radio button for the appropriate CA type being installed. Select the **Use custom settings to generate the key pair and CA certificate** check box and click the **Next** button to continue.



6. If a subordinate CA is selected, the CAs certificate must be obtained from a parent CA. Additionally, a certificate and CRL from the parent CA will be needed to complete the installation of the subordinate CA. Select the **Use custom settings to generate the key pair and CA certificate** check box and click the **Next** button to continue.

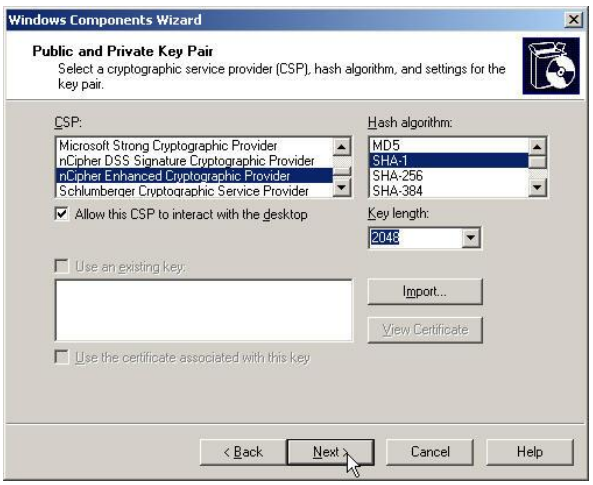


7. The **Public and Private Key Pair** dialog box of the **Windows Components Wizard** is displayed. In the **CSP** list box window of the **Public and Private Key Pair** dialog box, select the **nCipher Enhanced Cryptographic provider** option from the list of available cryptographic service providers. In the Hash algorithm list, select **SHA-1** (Secure Hash Algorithm version 1). Make sure that the **Use**

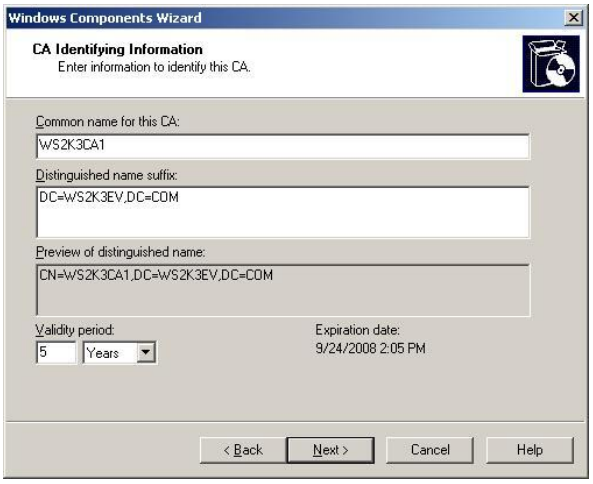
Copyright © 2008 Microsoft Corporation.

All rights reserved.

existing keys check box is cleared (not selected), and choose an appropriate key length in **the Key length** list box. It is recommended that a key length of at least 2048 be used. Check the **Allow this CSP to interact with the desktop** box. Click **Next**.



8. The **CA Identifying Information** dialog box is displayed. Enter the identifying information that is appropriate to the site and organization for which the CA is being implemented.



Note: The CA name (or common name) is critical; it is used to identify the CA object created in the directory.

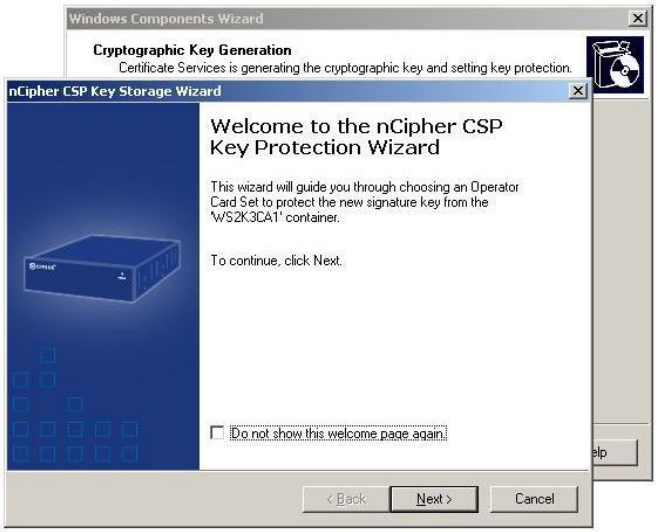
9. Validity periods can only be set for a root CA. Enter an appropriate time value in the **Validity period** box. If a subordinate CA is being installed, the validity period will be grayed out with a message stating **Determined by parent CA**.

Note: It is generally recommended that root CAs have a longer lifetime (such as 10 or 20 years) in comparison to an issuing CA that will be issuing end-entity certificates. Root certificates that are valid for a short duration require additional management because you must reissue root certificates to all of the client computers. The choice of a duration value is a trade-off between security and administrative overhead. Remember that each time a root certificate expires an administrator must update all of the trust relationships and "roll" the CA to a new certificate.

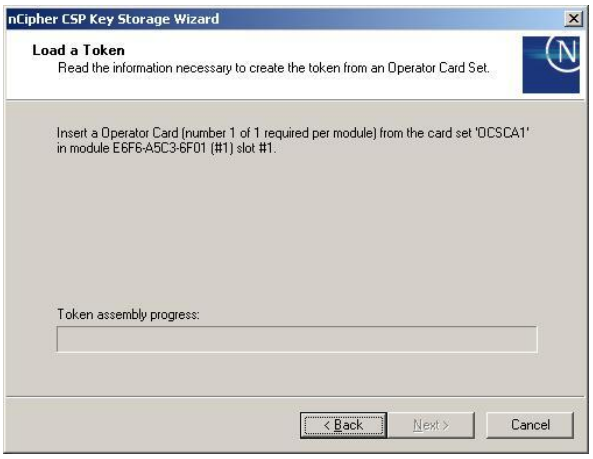
10. Click **Next** to continue. The **nCipher CSP Key Storage Wizard** panel appears. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



11. The **Load a token** panel appears. If the Operator Card is not in the smart card reader, the wizard will ask for it. Insert the Operator Card and click **Next** as required.



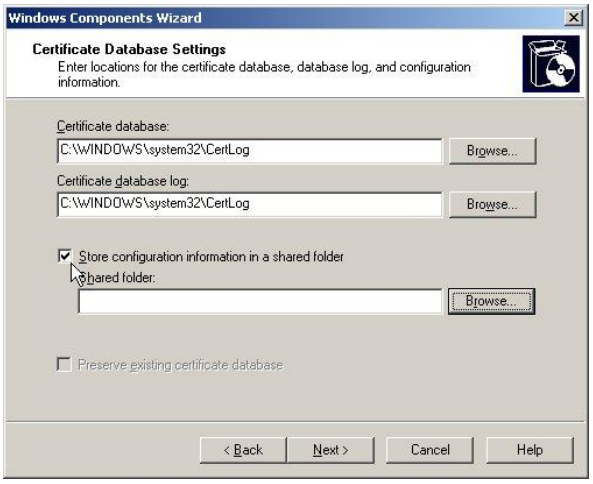
12. A panel appears indicating the **nCipher CSP Key Storage Wizard** setup is finished. Click **Finish**. Do not remove the operator smart card.

13. The **Certificate Database Settings** dialog box is displayed. This is where the locations of the certificate database, the configuration information, and the Certificate Revocation List (CRL) are

Copyright © 2008 Microsoft Corporation.

All rights reserved.

defined. Click to select the **Store configuration information in a shared folder** check box to specify the location of the folder where configuration information for the CA is stored. In the **Shared folder** box, type a Universal Naming Convention (UNC) path for this folder, and make sure that all of the CAs point to the same folder. Alternatively, click the **Browse** button to select a folder or create a new one. Click **Next** to continue.

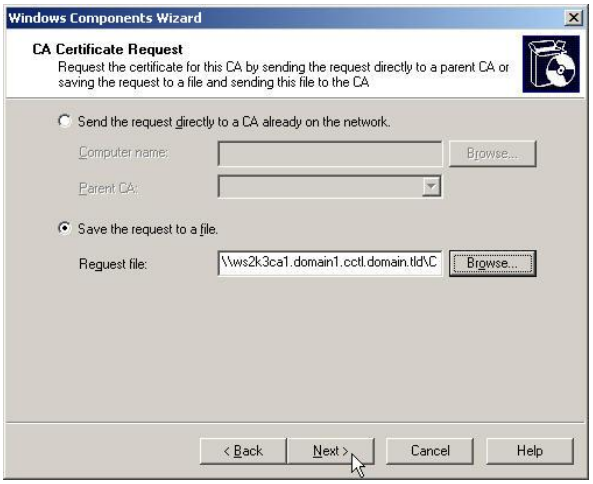


Note: Both New Technology File System (NTFS) and non-NTFS partitions are supported with Certificate Services. For the Evaluated Configuration, only NTFS partitions must be used. For CAs that will be used to issue high volumes of certificates, it is recommended that log files and the certificate database be placed on separate volumes for maximum performance. Actual performance characteristics will vary depending on hardware configuration and load placed on the certificate authority.

14. If installing a CA in the same location as a previously installed CA, the **Preserve existing certificate database** check box is selected by default. Click **Next**.

Warning: Do not select the **Preserve existing certificate database** check box if this is a new installation of the CA.

15. If installing an Enterprise Subordinate CA, the CA Certificate Request dialog box will be displayed. To obtain the certificate for a subordinate CA, a certificate request must be submitted to a parent CA. The procedure for doing so differs depending on whether the parent CA is available online.



a. If a parent CA is available online:

Copyright © 2008 Microsoft Corporation.
All rights reserved.

- Click **Send the request directly to a CA already on the network**.
- In **Computer Name**, type the name of the computer on which the parent CA is installed.
- In **Parent CA**, click the name of the parent CA.

b. If a parent CA is not available online:

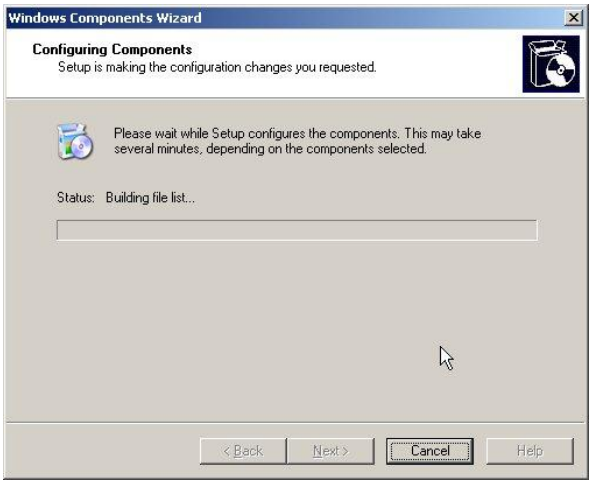
- Click **Save the request to a file**.
- In **Request file**, type the path and file name of the file that will store the request.
- Obtain this subordinate CA's certificate from the parent CA by taking the certificate request file to the offline parent CA.

Notes:

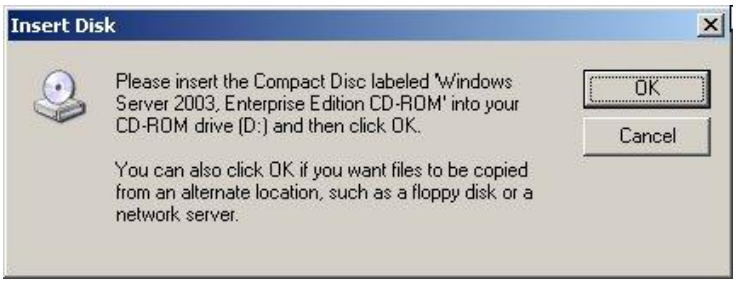
The procedure for doing this will be unique to the role of the parent CA. At a minimum, the parent CA should provide a file containing the subordinate CA's newly-issued certificate and, preferably, its full certification path.

If the subordinate CA certificate does not include the full certification path, the new subordinate CA being installed must be able to build a valid CA chain when it starts. Because of this, it is necessary to install the parent CA's certificate in the Intermediate Certification Authorities certificate store of the computer (if the parent CA is not a root CA), as well as the certificates of any other intermediate CA in the chain, and it is necessary to install the certificate of the root CA in the chain into the Trusted Root Certification Authorities store. These certificates should be installed in the certificate store before installing the CA certificate on the subordinate CA being set up.

16. The **Configuring Components** dialog box is displayed. Wait for the installation to finish.

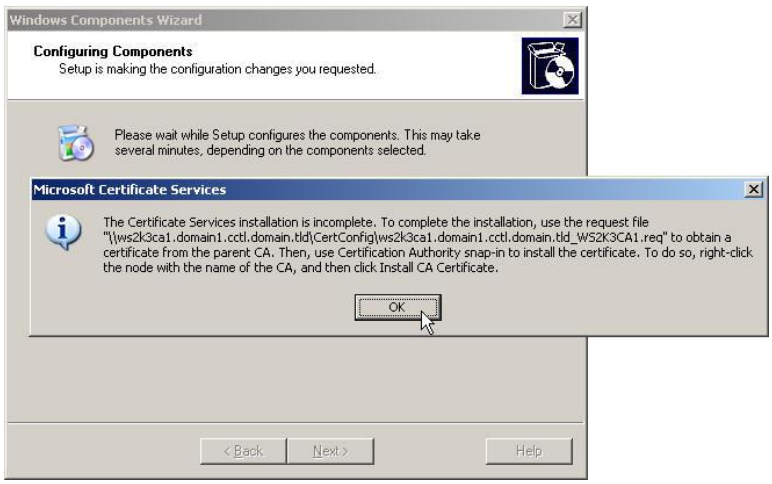


17. If the Windows Server 2003, Enterprise Edition media disk is not in the local CD-ROM drive, an **Insert Disk** message will appear. Insert the disk in the drive and click **OK** to continue configuring components. Cancel autoplay if necessary.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

18. If installing an Enterprise Subordinate CA with an offline parent CA, a message will appear indicating that the Certificate Services installation is incomplete. To complete the installation, the previously generated certificate request file must be used to obtain a certificate from the parent CA. Click **OK**.



19. If Internet Information Services is not installed or selected as a component for installation, a **Microsoft Certificate Services** message indicating that IIS is not installed will appear indicating that Certificate Services Web Enrollment Support will not be available until IIS is installed. Click **OK** to continue.

20. Click **Finish** to close the **Windows Components Wizard**.

21. Leave the Operator card in the smart card reader.
22. Close the **Add or Remove Programs** window.
23. The main portion of the CA installation is now complete.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Complete the installation of a subordinate CA associated with an offline parent CA

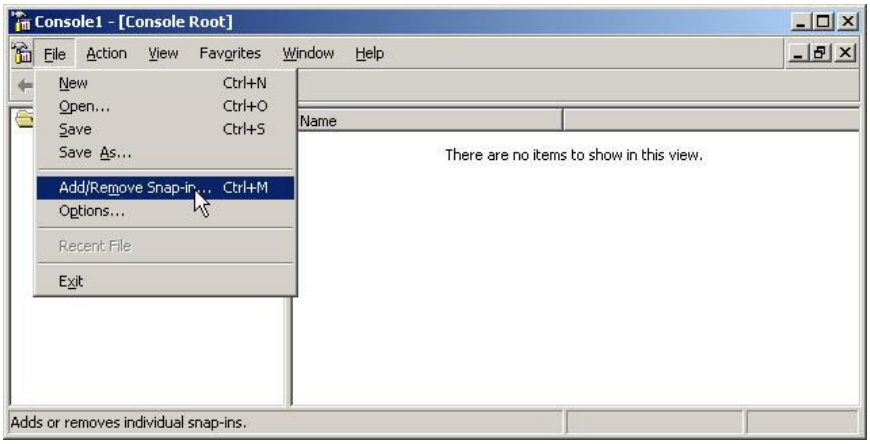
To complete the installation of a subordinate CA that has an offline parent CA, submit the certificate request file to the parent and have the parent CA issue a certificate to the subordinate. The following files will be needed from the parent CA in order to complete the installation of the subordinate CA:

- A copy of the parents CRL;
- A copy of the parent CAs public certificate; and
- An issued certificate for the subordinate CA.

Offline parent CAs can be part of the PKI environment, but are not part of the operating system TOE. Procedures for obtaining the files listed above are dependent on the type and management configuration of the offline parent CA that is used.

Install a CRL from a parent CA

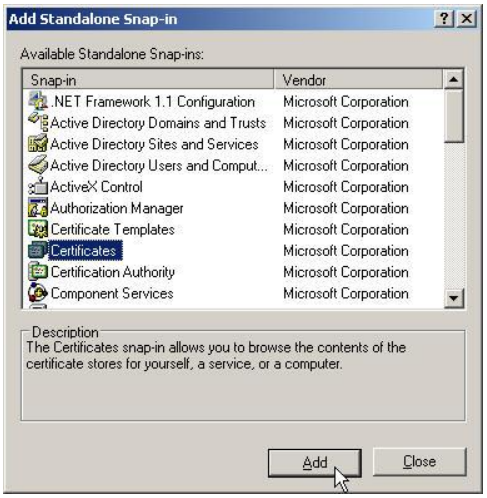
1. Log onto the subordinate CA as an authorized administrator.
2. Insert the media containing the parents CRL (floppy disk, CD-ROM, USB drive, etc.).
3. Open **Certificates** store for the local computer.
   - Click **Start**, select **Run**, type **mmc** in the run dialog box, and click **OK**.
   - Select **Add/Remove Snap-in** from the **File** menu.



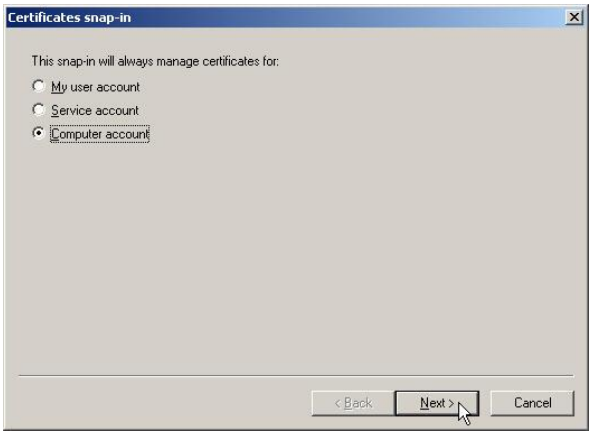
   - On the **Standalone** tab of the **Add/Remove Snap-in** interface, click the **Add** button.
   - Select **Certificates** from the **Add Standalone Snap-in** interface and click **Add**.

Copyright © 2008 Microsoft Corporation.

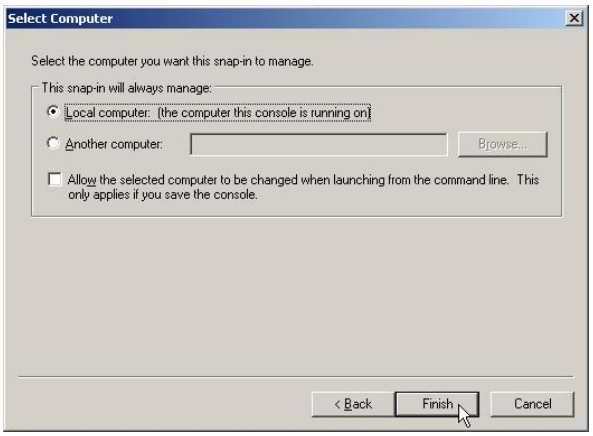
All rights reserved.



- Select the **Computer account** radio button in the **Certificates Snap-in** interface and click **Next**.



- Select the **Local computer (the computer the console is running on)** radio button in the **Select Computer** interface and click **Finish**.

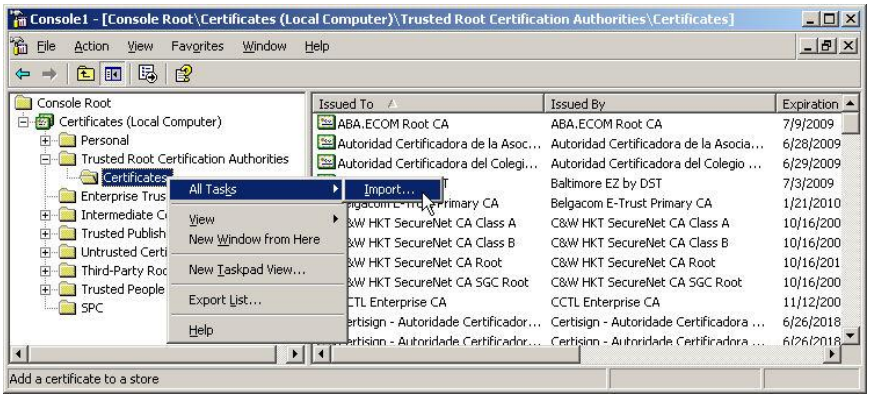


- Click **Close** on the **Add Standalone Snap-in** interface, and then click **OK** on the **Add/Remove Snap-in** interface.

4. Expand the **Certificates (Local Computer)** node in the interface and then expand the **Trusted Root Certification Authorities** folder. Right-click on the **Certificates** folder, point to **All Tasks**, and select **Import**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. The **Certificate Import Wizard** will appear. Click **Next**.

6. Click the **Browse** button on the **File to Import** page of the Wizard to locate the CRL file (it will have a .crl extension). The file will appear in the **File name** text box. Click **Next**.

7. Make sure the **Place all certificates in the following store** radio button is selected on the **Certificate Stores** page of the Wizard. The **Certificate store** text box should show the **Trusted Root Certification Authorities** store. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

8. Click **Finish** to complete the **Certificate Import Wizard**.

9. A message will appear indicating that the import was successful. Click **OK**.

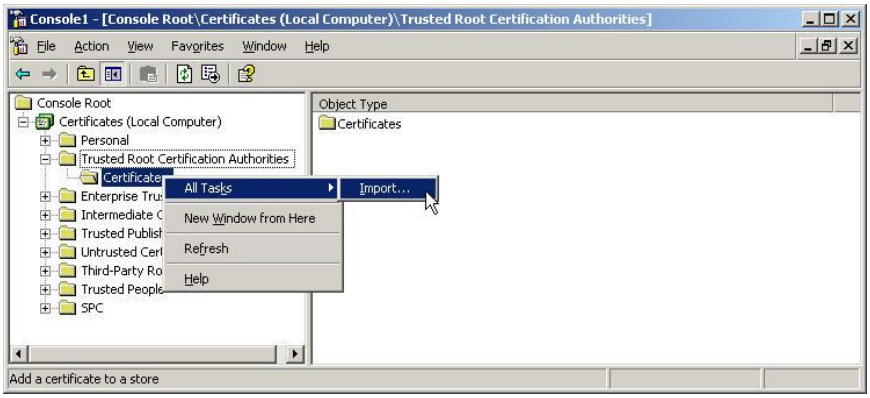
10. Leave the Certificates interface open to install the root CA certificate.

Install the parent CAs certificate

1. Expand the **Certificates (Local Computer)** node in the interface and then expand the **Trusted Root Certification Authorities** folder. Right-click on the **Certificates** folder, point to **All Tasks**, and select **Import**.

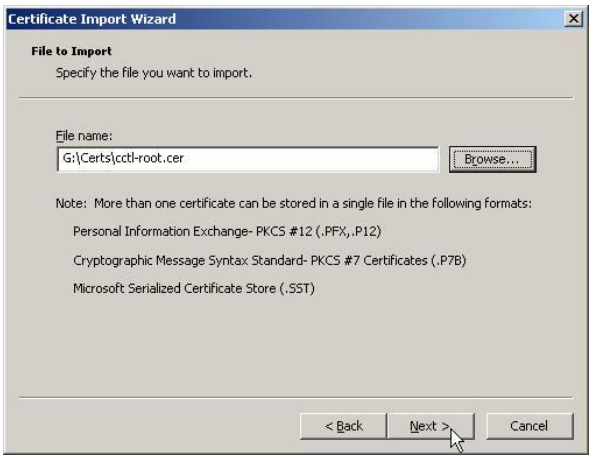
Copyright © 2008 Microsoft Corporation.

All rights reserved.



2. The **Certificate Import Wizard** will appear. Click **Next**.

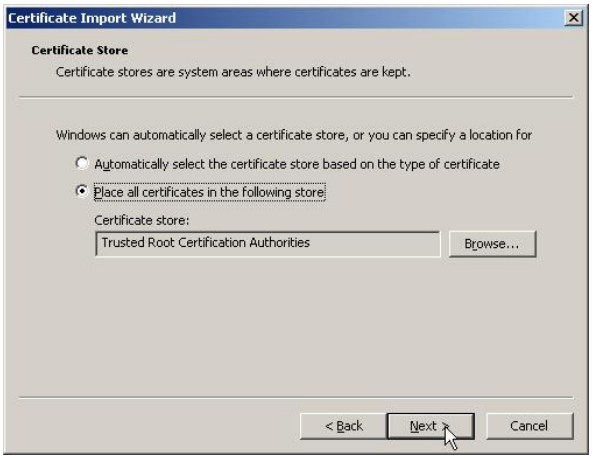
3. Click the **Browse** button on the **File to Import** page of the Wizard to locate the parent CAs certificate file (it will have a .cer extension). The file will appear in the **File name** text box. Click **Next**.



4. Make sure the **Place all certificates in the following store** radio button is selected on the **Certificate Stores** page of the Wizard. The **Certificate store** text box should show the **Trusted Root Certification Authorities** store. Click **Next**.

Copyright © 2008 Microsoft Corporation.

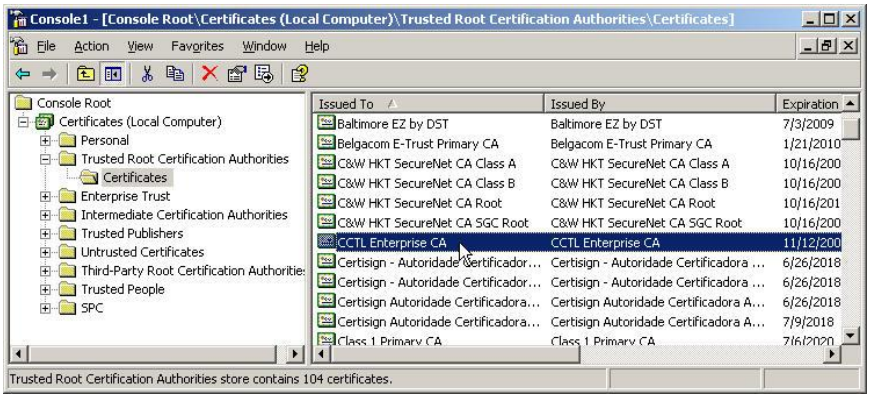
All rights reserved.



5. Click **Finish** to complete the **Certificate Import Wizard**.

6. A message will appear indicating that the import was successful. Click **OK**.

7. The parent CAs certificate will appear in the **Trusted Root Certification Authorities** store of the local computer.



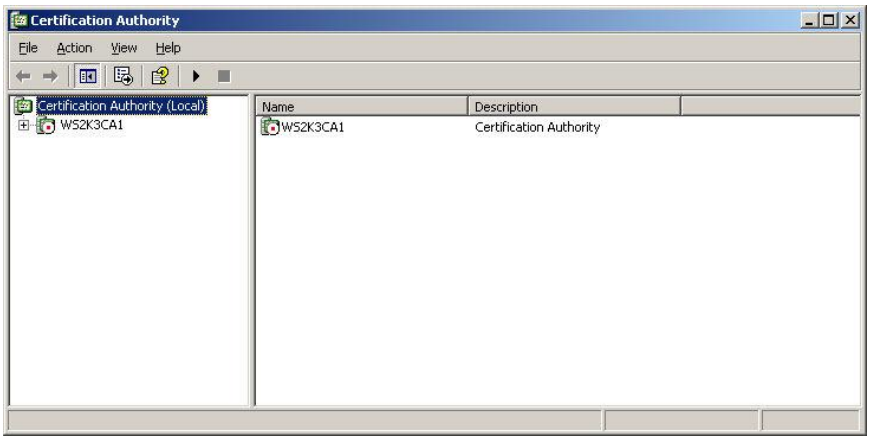
8. Close the Certificates interface and remain logged on to install the subordinate CAs certificate.

Copyright © 2008 Microsoft Corporation.

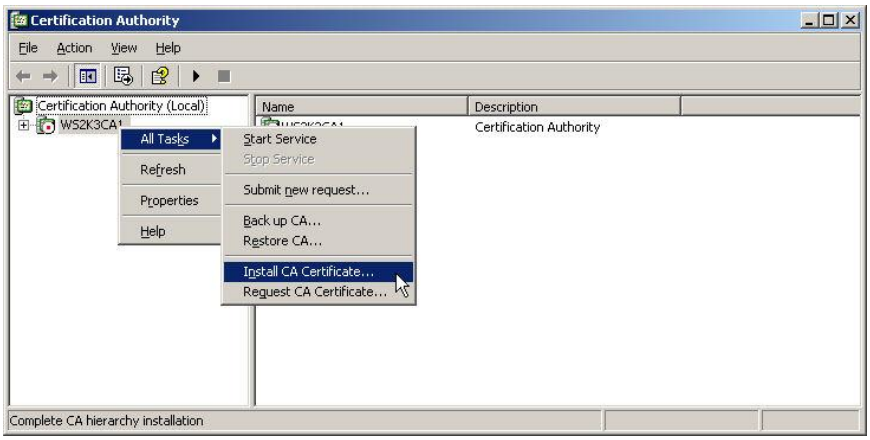
All rights reserved.

Install the subordinate CAs certificate

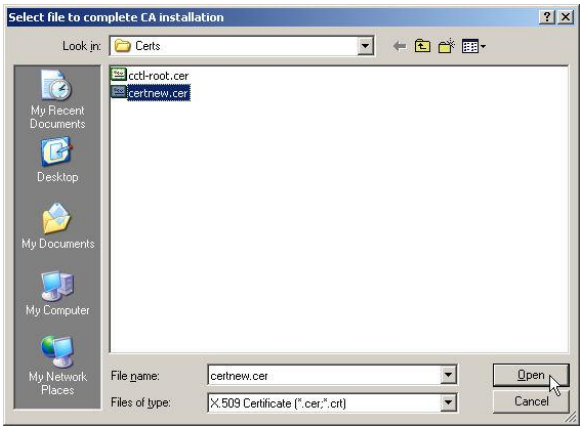
1. At the Subordinate CA, open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.



2. Right-click the node representing the CA, point to **All Tasks** and select **Install CA Certificate**.



3. Locate the certificate file received from the parent certification authority, select the file, and then click **Open**.



4. If the root CA is untrusted, click **OK** to trust the root CA's certificate.

5. Once the certificate is installed, start the **Certificate Services** service by right-clicking the node representing the CA, pointing to **All Tasks** and selecting **Start Service**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

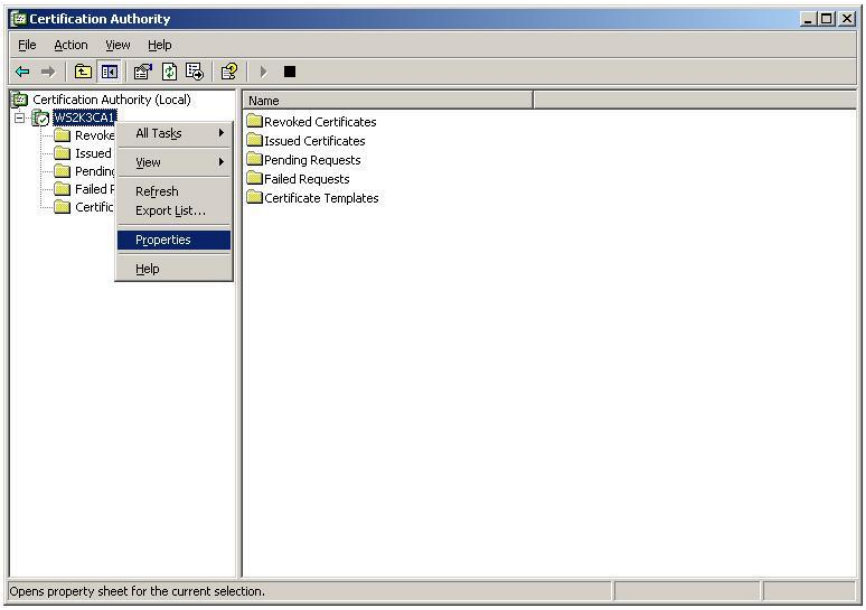
Add CRL Distribution Points and Authority Information Access Extensions to a Root CA

Follow the procedures below only if it is necessary to modify CRL Distribution Points (CDPs) or Authority Information Access (AIA) extensions for the CA. As previously mentioned, offline root CAs are outside the TOE but may be used to issue subordinate CA certificates to a CA within the TOE. To support this, the CRL distribution point information defined at the offline root CA must point to a location that is accessible by computers within the TOE. This is necessary because the offline root CA's default CDPs are not accessible to users within the TOE. If the root CA's CDP information is left unchanged, certificate revocation checking within the TOE will fail. If the root CA's AIA information is left unchanged, certificate chain verification will fail. Adding the root CA's certificate to the Trusted Root Certification Authorities Group Policy Setting in a domain will also support certificate chain verification.

Once the root CA's CDP and AIA information has been modified, a copy of the root CA's certificate and CRL must be placed in the location within the TOE environment that is specified in the CDP and AIA location information. For example, the path information for the root CA's CRL may be a shared folder on the Certificate Server host that is accessible by all users within the domain.

Note: This procedure applies to Root CAs only. Root CAs are typically maintained in an offline or disconnected state (a root CA residing within the TOE must use Active Directory and therefore cannot be maintained offline, however it may be disconnected). Therefore, CDPs and the AIA must be added so that applications can access CRLs and root CA certificates from an accessible location. Adding CDP and AIA extensions is an optional configuration for a CA.

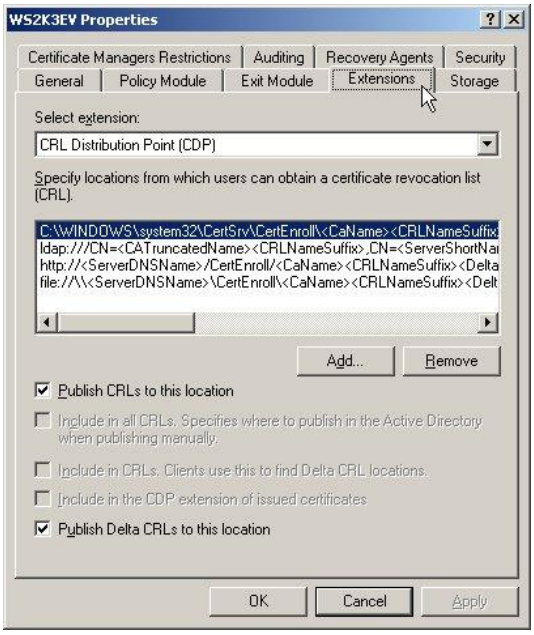
1. Open the **Certification Authority** interface for the recently installed Root CA. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
2. Right click the CA and select **Properties**.



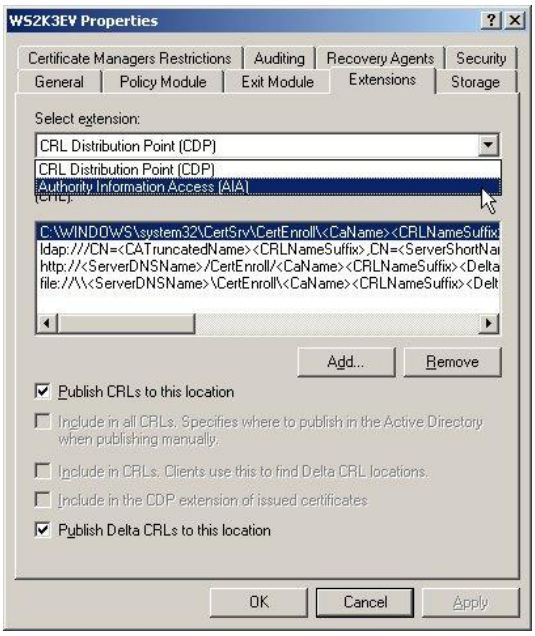
3. The Certification Authority's **Properties** interface will appear. Select the **Extensions** tab.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



4. Use the **Select Extension** drop-down menu to select between CRL and AIA, and then click the **Add** button to add a new location or the **Remove** button to remove an existing location.



Renewing the CA's Certificate

After the CDP and AIA extensions have been modified, the CA's certificate must be updated to reflect the new CDPs and AIAs. This process will vary slightly, depending on whether the CA is a root CA or a subordinate CA.

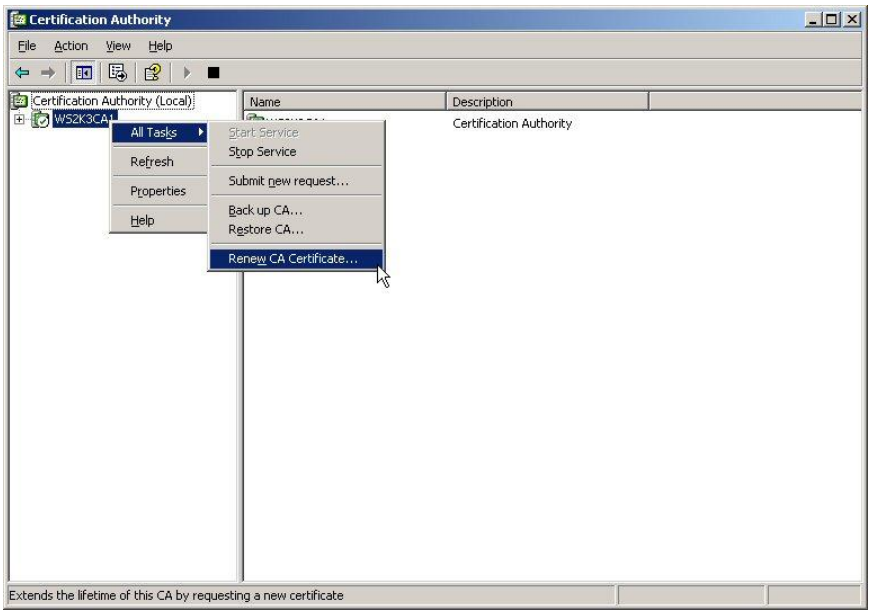
To renew a root CA's certificate:

1. Log on to the CA host as an authorized IT Administrator.

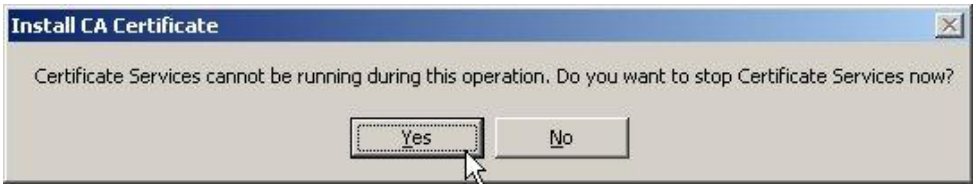
Copyright © 2008 Microsoft Corporation.

All rights reserved.

2. Open the **Certification Authority** interface for the Root CA. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right click the CA, select **All Tasks**, and then select **Renew CA Certificate**.



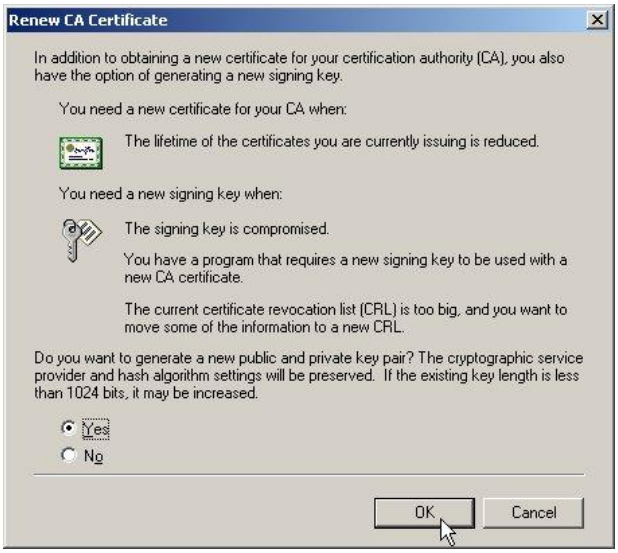
4. A message will appear stating that Certificate Services cannot be running during the renewal operations. Click **Yes** to stop Certificate Services.



5. A **Renew CA Certificate** interface will appear. It explains that in addition to generating a new CA certificate there is also an option of generating a new signing key. Read the information provided in the window to determine if a new signing key is required. If so, then select the **Yes** radio button and click **OK** to generate a new public and private key pair. If a new signing key is not required select the **No** radio button on the **Renew CA Certificate** interface and click **OK** to continue.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Note: If **Yes** is selected on the **Renew CA Certificate** interface, an additional message will appear asking if it is OK to overwrite the private key with a new one. If the **No** button is selected, the certificate renewal operation will be aborted. If the **Yes** button is selected, the renewal request operation will continue.

6. A new CA certificate will be generated and Certificate Services will be restarted. Close the **Certification Authority** interface if no further action is required.

To renew a subordinate CA's certificate:

1. Log on to the CA host as an authorized IT Administrator.
2. Open the **Certification Authority** interface for the Root CA. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right click the CA, select **All Tasks**, and then select **Renew CA Certificate**.
4. A message will appear stating that Certificate Services cannot be running during the renewal operations. Click **Yes** to stop Certificate Services.
5. A **Renew CA Certificate** interface will appear. It explains that in addition to generating a new CA certificate there is also an option of generating a new signing key. Read the information provided in the window to determine if a new signing key is required. If so, then select the **Yes** radio button and click **OK** to generate a new public and private key pair. If a new signing key is not required select the **No** radio button on the **Renew CA Certificate** interface and click **OK** to continue.

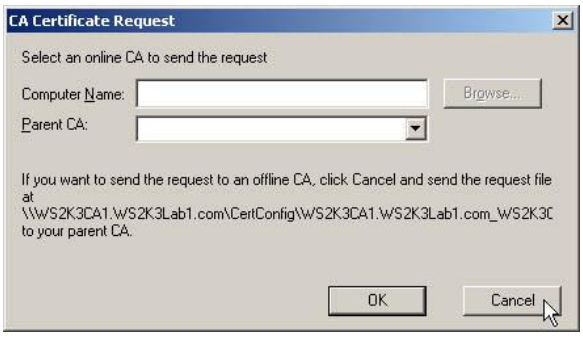
Note: If **Yes** is selected on the **Renew CA Certificate** interface, an additional message will appear asking if it is OK to overwrite the private key with a new one. If the **No** button is selected, the certificate renewal operation will be aborted. If the **Yes** button is selected, the renewal request operation will continue.

6. If the parent (or root) CA is online, the **CA Certificate Request** interface will show the parent CA's host path in the **Computer Name** text box. If this is not correct, or the online parent CA does not appear, select the **Browse** button to find the parent CA on the network. The parent CA will be shown in the **Parent CA** box. If this is not correct, select the parent CA from the drop-down menu after entering the host name in the **Computer Name** text box. Click **OK**. Certificate Services will be restarted. Close the **Certification Authority** interface if no further action is required.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

7. If the parent (or root) CA is offline, the **CA Certificate Request** interface will not show the parent CA in the **Computer Name** text box and there will be no selections in the Parent CA drop down menu. The **Browse** button will be grayed out if no CA are detected on the network. Note the path to the request file that is specified in the **CA Certificate Request** interface and click **Cancel**. Certificate Services will be restarted. Continue with Steps 8 and 9 to obtain and install the new subordinate CA certificate received from an offline CA.



8. Obtain this subordinate CA's certificate from the parent CA by taking the certificate request file to the offline parent CA and obtaining the new subordinate CA certificate. Also obtain a new CRL if necessary.
9. Follow the procedures in the Install a CRL from a parent CA and Install the subordinate CAs certificate subsections.

Trusted Root Certification Authorities Group Policy Settings

When an Enterprise root CA is installed, the certificate of the CA is added automatically to the **Trusted Root Certification Authorities** Group Policy object for the domain. Domain Administrators can also add certificates for other root CAs (such as an offline root CA certificate) to the **Trusted Root Certification Authorities** Group Policy object.

The root CA certificates that are added become trusted root CAs for computers within the scope of the Group Policy object.

Verify that the root CA's certificate is added to the **Trusted Root Certification Authorities** Group Policy object for the domain, or add it if required, by following the procedures below.

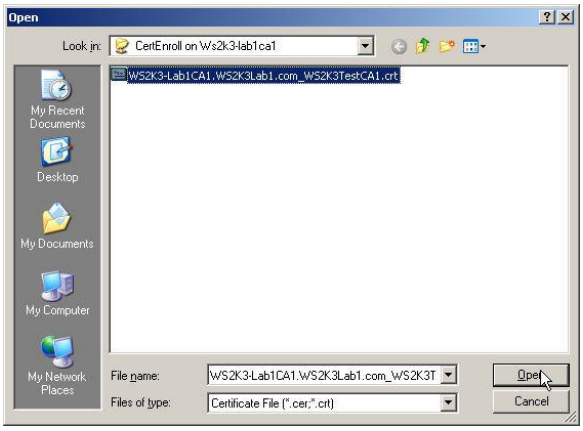
1. Log on to a Domain Controller as an authorized domain administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Domain Security Policy**.
3. Expand the **Public Key Policies** folder and select **Trusted Root Certification Authorities**.
4. Verify that the root CA's certificate is shown in the right-hand details pane.

Copyright © 2008 Microsoft Corporation.
All rights reserved.

5. If the root CA's certificate is not shown in the right-hand details pane, right-click on the **Trusted Root Certification Authorities** folder and select **Import**. The Certificate Import Wizard will appear. Click **Next**.

6. In the **File to Import** view of the Wizard, click the **Browse** button.
7. If the CA is online, browse to the share location containing the root CA's certificate. If the CA is offline, insert the media containing the CA's certificate and browse to that location.

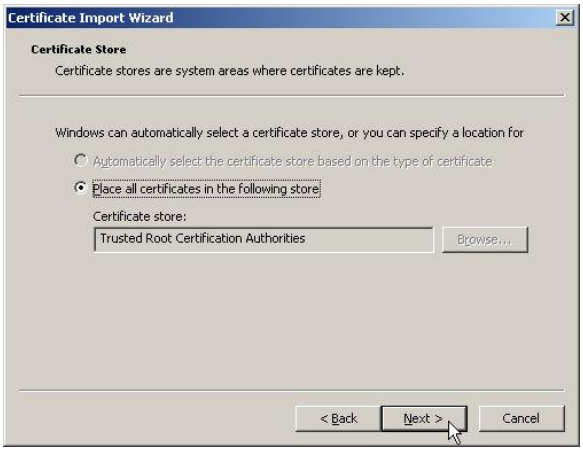
Note: If the CA is offline, its certificate must first be obtained directly from the CA and brought back to the Domain Controller to proceed with this procedure.



8. Click **Next** on the **File to Import** view of the Wizard.
9. Click **Next** on the **Certificate Store** view of the Wizard. It should show **Trusted Root Certification Authorities** as the **Certificate store**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



10. Click Finish to complete the Wizard. A message will appear indicating that the import was successful. Click **OK**

11. The certificate will now appear in the **Trusted Root Certification Authorities** folder of the Domain Security Policy and will be accessible to all domain hosts.

Adjusting the Clock Skew Registry Settings

The **ClockSkewMinutes** registry value controls the time variance allowed for certificate issuance, certificates, and CRLs. If the times on the clocks on two computers are further apart than this registry setting, a newly enrolled certificate would not be immediately valid and the client would have to wait several minutes before being able to use the new certificate. The default setting is 10 minutes, however, for the Evaluated Configuration this setting must be changed to 1 minute.

To verify the ClockSkewMinutes registry setting:

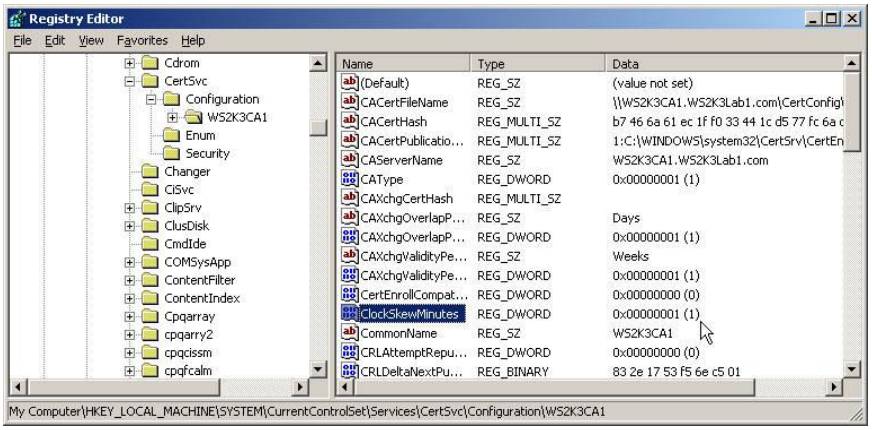
1. Log on to the computer as an authorized Administrator.
2. Click **Start** and select **Run**. Type **regedit** and click **OK**.
3. Navigate the **Registry Editor** to find and select the following key path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CAName>

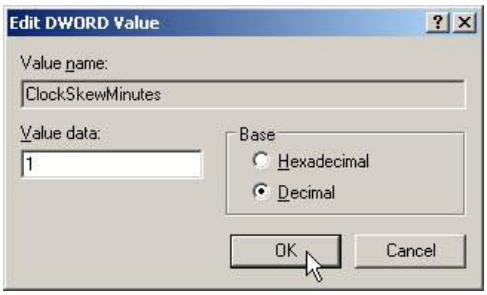
4. Verify that the **ClockSkewMinutes** value is set to **1** minute.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. If the value needs to be modified, double-click on the **ClockSkewMinutes** registry value. On the **Edit DWORD Value** interface, select the **Decimal** radio button, enter a **1** in the Value data field and click **OK**.



Copyright © 2008 Microsoft Corporation.

All rights reserved.

Configuration of Certificate Server Management Roles

Role-based administration involves the use of explicitly assigned CA management roles. To assign a CA management role to a user or group, the corresponding security permissions or user rights that define each role must be assigned to the selected accounts in order to grant them the explicit capabilities assigned to a role. Table A-3 describes the CA management roles relevant to Windows Server 2003 Certificate Server role-based administration.

Table A-3 CA Management and User Roles

Role	Required CA Security Permissions / User Rights / Group Membership	Description
CA Administrator	**CA Security Permissions:** (Applied through the CA properties interface) Allow **Manage CA** permission.	Configures and maintains the CA. This is a CA management role defined through CA specific security permissions.
Certificate Manager (Also known as the Officer role)	**CA Security Permissions:** (Applied through the CA properties interface) Allow **Issue and Manage Certificates** permission.	Approves certificate enrollment and revocation requests. This is a CA management role defined through CA specific security permissions. This role is sometimes referred to as CA Officer.
CA Backup Operator	**Group Membership:** (Default built-in group on CA host) Add to **Backup Operators** group. (provides **Back up file and directories** and **Restore file and directories** privileges).	Performs CA system backup and recovery. This is a CA management role defined through operating system based user rights assignment.
CA Auditor	**User Rights:** (Local user right on CA host) Grant Manage auditing and security log privilege.	Configure, view, and maintain audit logs. This is a CA management role defined through operating system based user rights assignment.
Enrollee	**CA Security Permissions:** (Applied to the Authenticated Users group through the CA properties interface) Allow **Request Certificates** permission.	Enrollees are clients authorized to request certificates from the CA. By default, the Authenticated Users group is assigned the Enrollee role and no changes need to be made for this role. This is not a CA management role, but is required to ensure that users within the organization can make certificate requests.

Define Authorized Accounts for CA Management Roles

Before proceeding with the assignment of CA management roles, make sure that specific user accounts have been identified/created for each role. To facilitate CA management role administration, it is recommended that special group accounts be created to support the CA Administrator, Certificate Manager, CA Backup Operator, and CA Auditor roles. At the domain level, global group accounts can be created to support role assignments for specific CAs. The global groups can then become members of corresponding CA group accounts on the local CA host. To grant or remove CA role assignments to domain user accounts, the accounts can be added or removed from the CA global group accounts as required.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The rights and permissions granted to CA roles are controlled at the CA host via permissions and user rights granted to the global or local CA groups. For example a group called CA Auditors can be created on the CA host and assigned the local **Manage auditing and security log** privilege. The Backup Operators group already exists by default in the Windows Server 2003 operating system and can be used to grant CA Backup Operator rights. Corresponding security permissions or user rights can then be assigned to each group account based on the CA management role it is to support. User accounts which have been authorized to serve as CA managers are placed in the appropriate global group to support each specific role. User accounts must not be assigned to more than one CA management role and CA management roles should only be assigned to group accounts and not individual user accounts. Additionally, group accounts that have been assigned CA Administrator or Certificate Manager roles must not be members of the local Administrators, Domain Admins, or Enterprise Admins security groups. Procedures for configuring each group account to support a CA management role are defined in the subsections that follow. Table A-4 provides recommendations for creating global and local groups to support CA management roles.

Note: Procedures for creating user accounts and group accounts in Windows Server 2003 can be found in the Creating and Maintaining User and Group Accounts subsection of this document.

Table A-4 Recommendations for Domain and Local CA Management Groups

Supported Roles	Domain Global Groups	Local Groups on CA Host
CA Administrator	***<CA Name>* Admins** **Members:** Add domain users that have been designated as authorized CA Administrators for the specified CA. **Member of:** Local ***CA Admins*** group on the computer hosting the CA.	**CA Admins** **Members: *<CA Name>* Admins** global group.
Certificate Manager (Also known as the Officer role)	***<CA Name>* Cert Managers** **Members:** Add domain users that have been designated as authorized Certificate Managers for the specified CA. **Member of:** Local ***CA Cert Managers*** group on the computer hosting the CA.	**CA Cert Managers** **Members: *<CA Name>* Cert Managers** global group.
CA Backup Operator	***<CA Name>* Backup Operators** **Members:** Add domain users that have been designated as authorized CA Backup Operators for the specified CA. **Member of:** Local ***CA Backup Operators*** group on the computer hosting the CA.	**Backup Operators** (Default built-in group on CA host) **Members: *<CA Name>* Backup Operators** global group.
CA Auditor	***<CA Name>* Auditors** **Members:** Add domain users that have been designated as authorized CA Auditors (CA audit administrators) for the specified CA. **Member of:** Local ***CA Auditors*** group on the computer hosting the CA.	**CA Auditors** **Members: *<CA Name>* Auditors** global group.

Copyright © 2008 Microsoft Corporation.

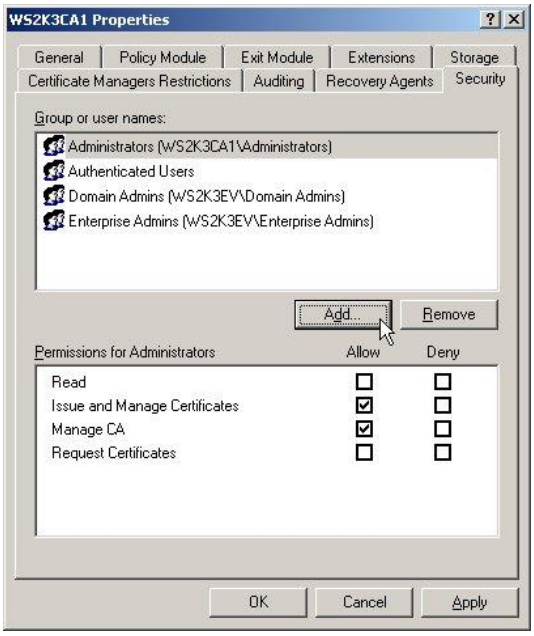
All rights reserved.

Assign CA Administrator Role

The CA Administrator role is used to manage the CA and applies only to specific tasks within the functionality of the CA. It can configure and maintain the Certificate Server. This includes the ability to assign all other CA management roles and renew the CA certificate. CA Administrators are designated by assigning the **Manage CA** permission in the **Certification Authority** interface.

The CA Administrator role is not to be confused with that of the local administrator for the host operating system or for any of the network administrative accounts. The local Administrator applies to the local operating system privilege which may be required to perform some administrative tasks associated with the operations of the CA. The local Administrator will always have full control of the system including the CA and cannot be blocked from taking control of the CA since the local Administrator can modify account privileges and group memberships within the operating system. As a matter of local policy and best security practice, basic administration of the Certification Authority must only be done through a CA Administrator role which does not have local operating system administrative privileges. Assign the CA Administrator role to the group account authorized for this role as follows:

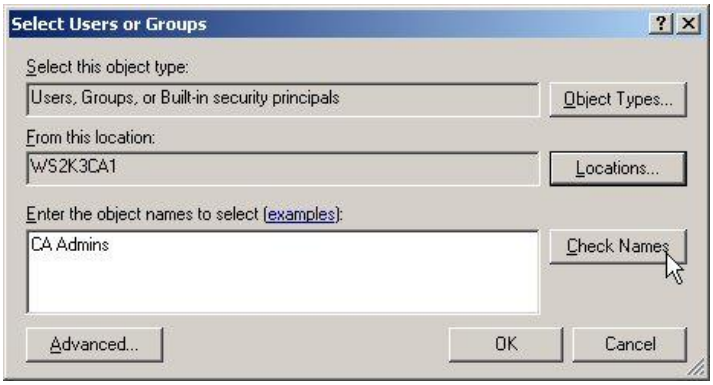
1. Log on as an authorized administrator.
2. Open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right-click the CA node and select **Properties**. The **Properties** interface for the CA will appear. Click on the **Security** tab to bring it to the foreground. Click the **Add** button.



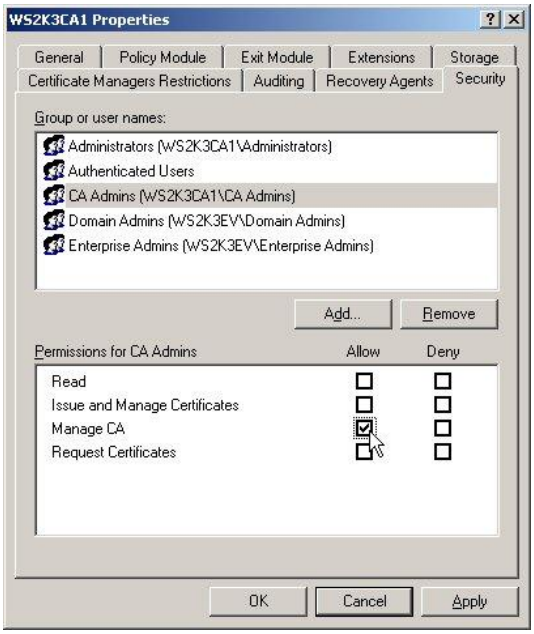
4. The **Select Users, Computers, or Groups** dialog box will appear. If necessary, find and set the location of the CA management group roles by using the **Locations** button. In the **Enter the object names to select** text box, enter the name of the pre-defined group account that is to be assigned to the CA Administrator role. If necessary, click the **Check Names** button to verify that the account exists. Click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. The account will appear in the **Group or user names** box. Highlight the account by selecting it. In the **Permissions for <user name>** window, check the **Allow** box for the **Manage CA** permission and uncheck the **Allow** box for **Request Certificates**.



6. Click the **Apply** button. If no further roles are to be configured click the **OK** button to close the **Properties** interface for the CA.

Assign Certificate Manager Role

The Certificate Manager role is distinctly different from that of the CA Administrator role in that it is solely responsible for managing the approval or disapproval of certificate enrollment and revocation requests. Certificate Managers can also submit certificate requests on behalf of users. Certificate Managers are designated by assigning the **Issue and Manage Certificates** permission in the **Certification Authority** interface.

Note: To submit certificate requests on behalf of users, the account that is to be assigned to the Certificate Manager role must have an Enrollment Agent certificate. For the Evaluated Configuration, Enrollment Agent certificates must only be granted to accounts that are assigned to the Certificate Manager role. Procedures for modifying and assigning an Enrollment Agent certificate are demonstrated in the Smart Card Deployment subsection of this document.

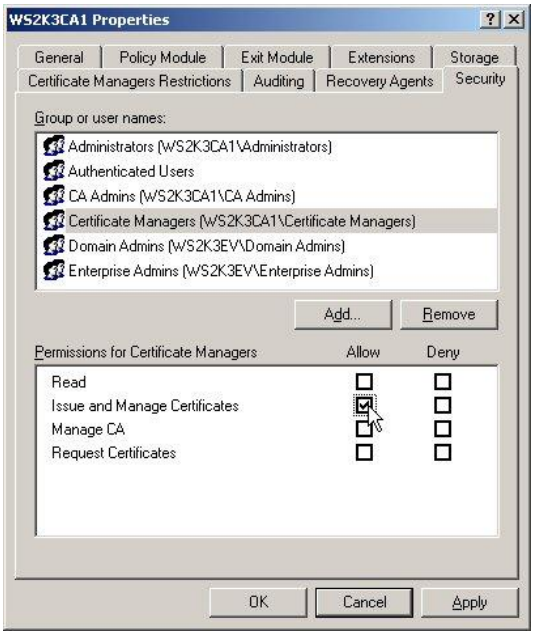
Copyright © 2008 Microsoft Corporation.

All rights reserved.

Assign the CA Administrator role to the group account authorized for this role as follows:

1. Log on as an authorized administrator.
2. Open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right-click the CA node and select **Properties**. The **Properties** interface for the CA will appear. Click on the **Security** tab to bring it to the foreground.
4. Click the **Add** button. The **Select Users, Computers, or Groups** dialog box will appear. Enter the name of the pre-defined group account that is to be assigned to the Certificate Manager role. If necessary, click the **Check Names** button to verify that the account exists. Click **OK**.

5. The account will appear in the **Group or user names** box. Highlight the account by selecting it. In the **Permissions for <user name>** window, check the **Allow** box for the **Issue and Manage Certificates** permission and uncheck the **Allow** box for **Request Certificates**.



6. Click the **Apply** button. If no further roles are to be configured click the **OK** button to close the **Properties** interface for the CA.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Assign CA Backup Operator Role

The CA Backup Operators are responsible for backup and restoration of the Certificate Server. Like the CA Auditor role, this role is not assigned directly through the **Certification Authority** interface. Instead, the authorized user or group account for this role must be added to the Windows Server 2003 built-in **Backup Operators** group. This will allow the designated account access to the backup and restore features of the **Certification Authority** interface. Procedures for adding accounts to a group are available in the Creating and Maintaining User and Group Accounts subsection of this document.

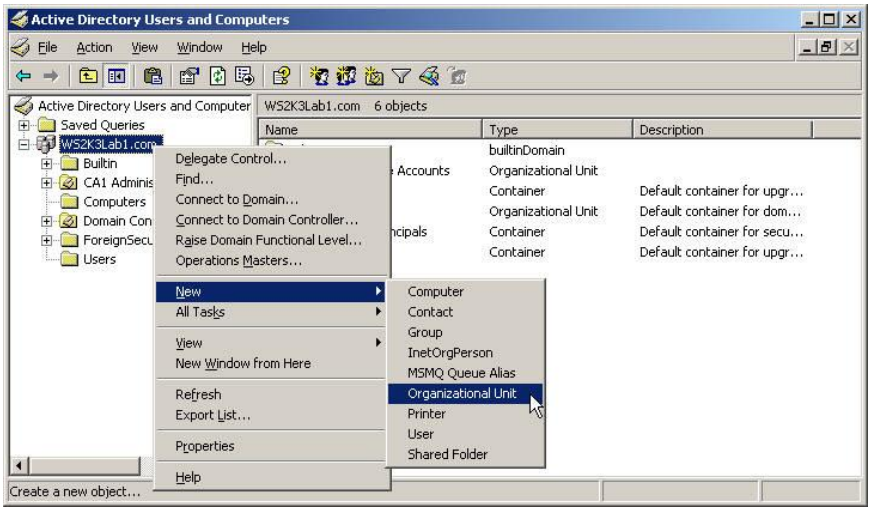
Assign CA Auditor Role

CA Auditors manage the auditing aspects of the Certificate Server. This role is not assigned directly through the **Certification Authority** interface. Instead, the **Manage auditing and security log** user right needs to be assigned to the authorized user or group account designated for the CA Auditors role. This will allow the designated account to access the audit management features of the **Certification Authority** interface and to view and sort through the audit events in the **Event Viewer** interface. Detailed procedures for assigning user rights and privileges to user and group accounts are available in the Configuring User Rights subsection of this document.

If a Domain Security Policy is in place, it may prevent modifications to this setting in the Local Security Policy of the CA host. In such a case, it may be necessary to create a special Group Policy in the domain for the CA. The **Manage auditing and security log** user right setting can be modified in the CA Group Policy and will take precedence over the settings in the Domain Security Policy.

To create a group policy for a CA in a domain, first create a new organizational unit (OU) for the CA in **Active Directory Users and Computers** and then move the CA host computer object from the **Computers** folder and into the new OU. Now a group policy can be created for the new organizational unit and its settings will be applied to the CA host computer.

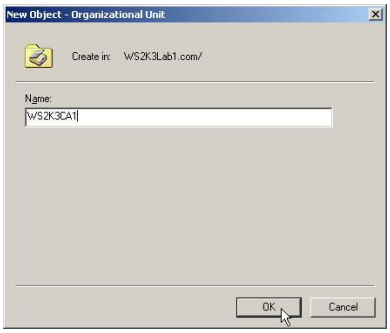
1. Log on to a Domain Controller as an authorized domain administrator.
2. Click **Start**, point to **Administrative Tools**, and select **Active Directory Users and Computers**.
3. Right-click on the domain node, point to **New**, and select **Organizational Unit**.



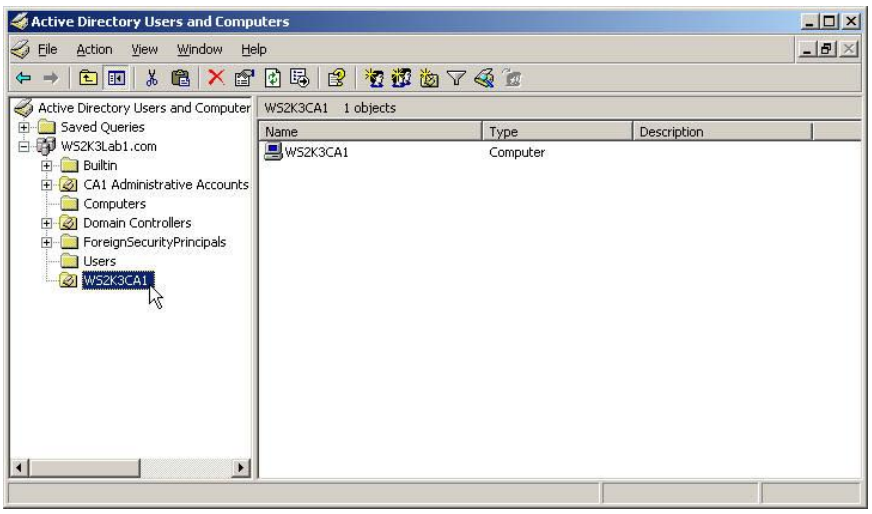
4. In the **New Object – Organizational Unit** interface, enter the name for the OU, and then click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



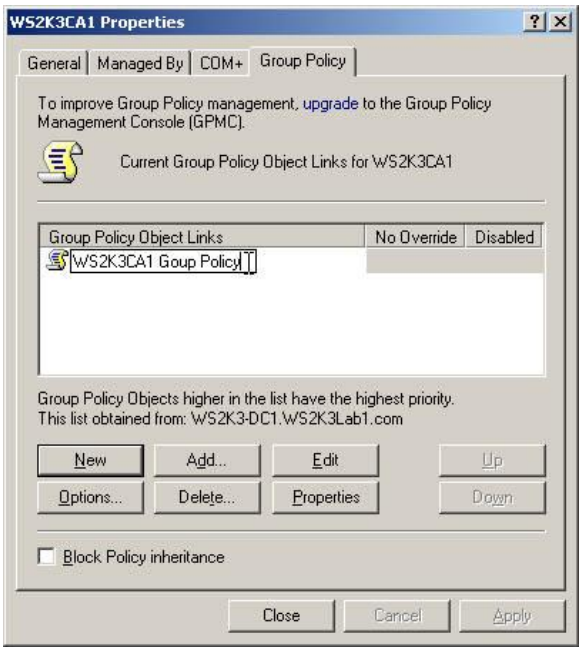
5. Select the **Computers** folder, then drag and drop the CA computer object from the **Computers** folder and into the new OU folder. A message will appear, warning about moving objects in Active Directory, click **Yes**. The CA computer object will now appear in the new OU.



6. Right-click on the OU folder and select **Properties**.
7. Select the **Group Policy** tab and then click the **New** button.
8. A **New Group Policy Object** will appear in the **Group Policy Object Links** window. Change the name to reflect the new policy for the CA.

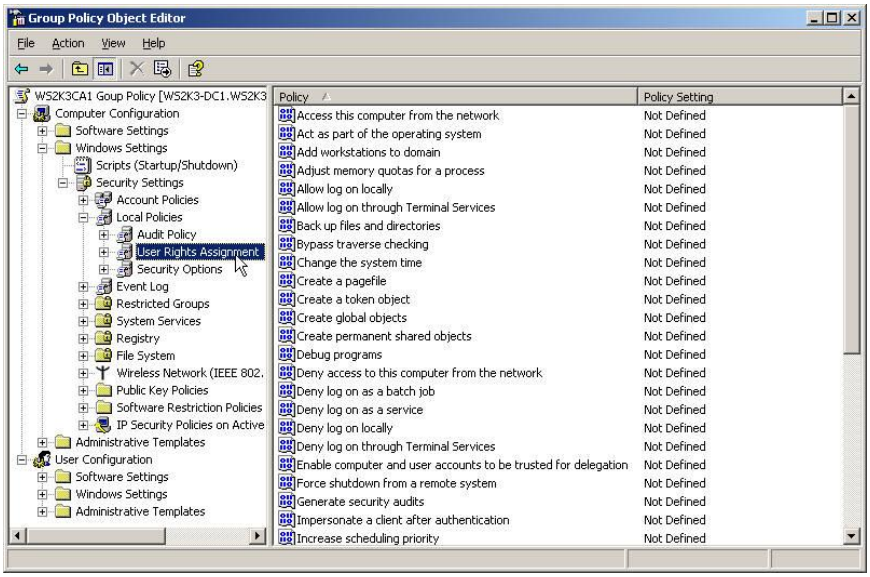
Copyright © 2008 Microsoft Corporation.

All rights reserved.



9. Select the new Group Policy and click the **Edit** button. The **Group Policy Object Editor** interface will appear.

10. Under **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then select **User Rights Assignment**.



11. On the right-hand details pane, double-click on the **Manage auditing and security log** policy setting.

12. In the **Manage auditing and security log Properties** interface, check the **Define these policy settings** check box, and then click **Add User or Group**.

13. Click **Browse** on the **Add User or Group** interface. Then click **Advanced** in the **Select Users, Computers, or Groups** interface, and then click **Find Now**.

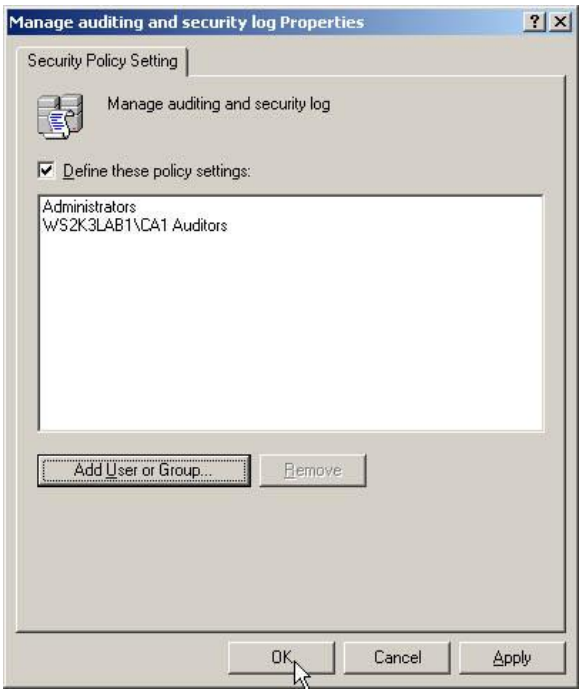
14. Select the group designated for CA Auditor roles and click **OK**.

15. Click **Advanced** one more time, and click **Find Now**. Select the Administrators group and click **OK**. Click **OK** on the next two interfaces.

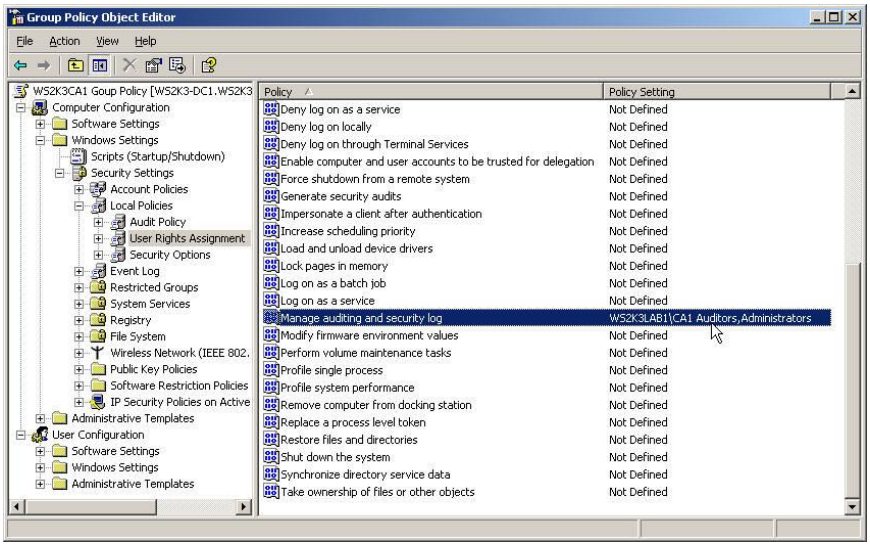
Copyright © 2008 Microsoft Corporation.

All rights reserved.

16. Click **OK** on the **Manage auditing and security log Properties** interface.



17. The **Group Policy Object Editor** interface will show that the designated CA auditors group and the Administrators group are granted the **Manage auditing and security log** privilege.



18. Do not change any other policy settings. Close the **Group Policy Object Editor** interface, and then click **Close** on the OU **Properties** interface.

19. The new group policy will only modify the **Manage auditing and security log** privilege on the CA host.

Note: Group policies update automatically every 15 minutes. To force an immediate update, execute **gpupdate /force** from a command prompt.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Set Administrative Tools Menu for CA Management Roles

To perform functions designated for each of the CA management roles, the users assigned to these roles must be able to access the **Certification Authority** interface from the **Administrative Tools** menu. However, since the accounts selected to manage the CA do not have local system administrator rights, when those users log on to the CA their start menu will not display a selection for **Administrative Tools**. The procedures below are used to set the **Administrative Tools** menu for each of the accounts that are assigned to one of the CA management roles.

1. Log on using an account that has been assigned one of the CA management roles.
2. Right-click **Start** and select **Properties**. The **Taskbar and Start Menu Properties** interface will appear.
3. From the **Start Menu** tab view, select the **Start menu** radio button and click the **Customize** button that is next to it. The **Customize Start Menu** interface will appear.
4. Select the **Advanced** tab.
5. In the **Start menu items** dialog window, scroll to **System Administrative Tools** (last item in the list).
6. Select either the **Display on the All Programs menu** or the **Display on the All Programs menu and Start menu** radio button.
7. Click the **OK** button on the **Customize Start Menu** interface.
8. Click the **OK** button on the **Taskbar and Start Menu Properties** interface.

Remove Default Accounts from CA Management Roles

The default installation setting for an Enterprise CA is to have local Administrators, Enterprise Admins, and Domain Admins as CA Administrators. To limit the power of any of these accounts, they must be removed from the CA Administrator and Certificate Manager roles once all CA management roles have been properly assigned. Keep in mind that although this will result in limiting the local Administrator account's ability to directly manage the CA, the local Administrator will always have full control of the system and cannot be directly prevented from making modifications that would allow full control of the CA. Therefore, it is necessary that, along with the modifications to the CA management roles, organizations follow strict procedural policies for maintaining a separation of responsibilities between CA management roles and those of the local system administrators.

1. Log on the computer hosting the Certificate Server using an account that has been authorized for the CA Administrator role.
2. Open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right-click the CA node and select **Properties**. The **Properties** interface for the CA will appear. Click on the **Security** tab to bring it to the foreground.
4. Select the **Administrators** account from the **Group or user names** box and click the **Remove** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

5. If the **Domain Admins** and **Enterprise Admins** accounts are present, remove them as well.

6. Click the **OK** button to close the **Properties** interface for the CA.

Set Template Permissions and Ownership

After configuring the CA management roles, the Domain Administrator will need to grant the account representing the CA Administrator role the ability to make modifications to certificate templates. To modify certificate templates, the CA Administrator role will need both access permissions to the templates and ownership of the templates. Although permission and ownership changes can be made to the default templates, the ownership will revert back to Enterprise Admins whenever the templates interface is accessed by an Enterprise Administrator. To prevent this from occurring, it is necessary to make duplicates of all the certificate templates that will be managed by the CA Administrator and then set the

Copyright © 2008 Microsoft Corporation.

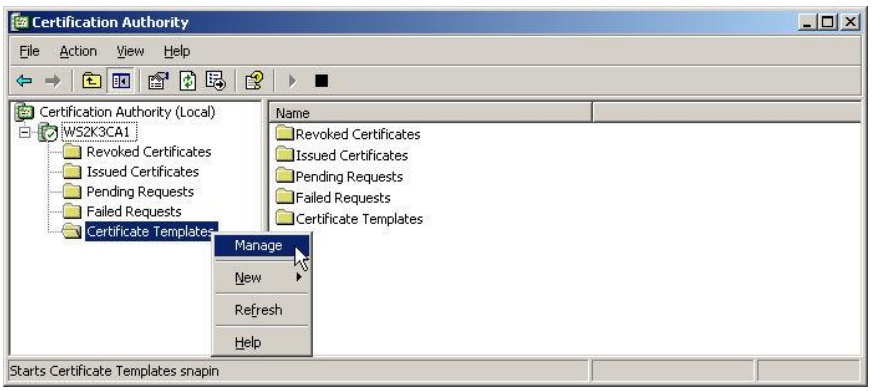
All rights reserved.

permissions and ownership as required. The ownership of duplicate templates will not change when accessed with domain or enterprise level administrative rights.

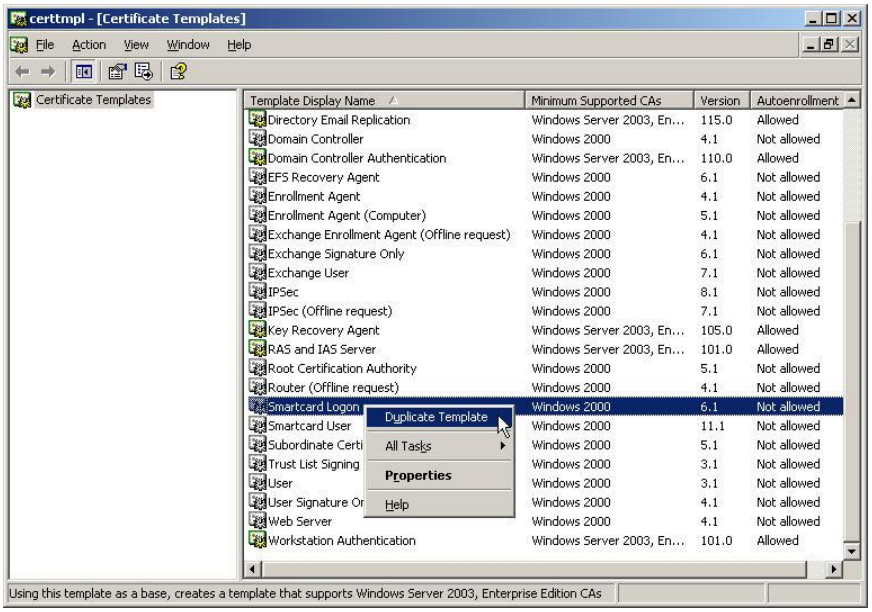
Note: If a duplicate template is replacing a template previously available for issuance, the new duplicate template should be configured to supersede the previous template version. Procedures for superseding templates are available in the "Superseded Templates" subsection of Appendix B.

To create duplicate certificate templates:

1. Log on to the computer as a Domain or Enterprise Administrator.
2. Open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Expand the CA node, then right-click on the **Certificate Template** folder and select **Manage**.



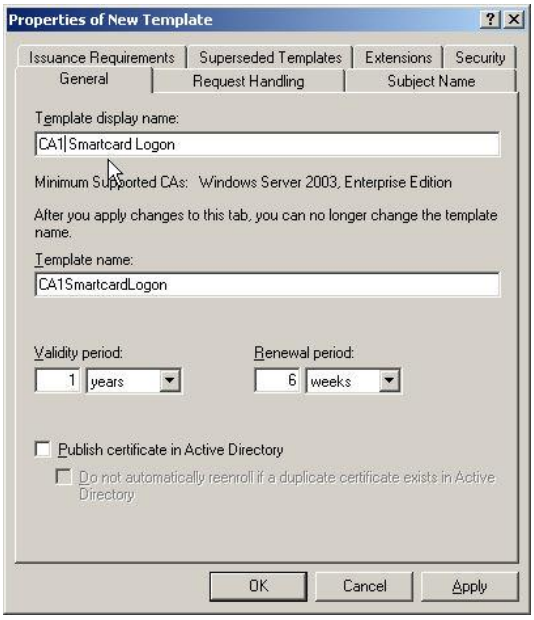
4. The **Certificate Templates** interface will appear. On the right-hand details pane, right-click on a template that is to be duplicated and select **Duplicate Template**.



5. A **Properties of New Template** interface will appear. Make appropriate changes to the template display name. Do not make other changes to the duplicate template at this time. Click **OK** to close the template.

Copyright © 2008 Microsoft Corporation.

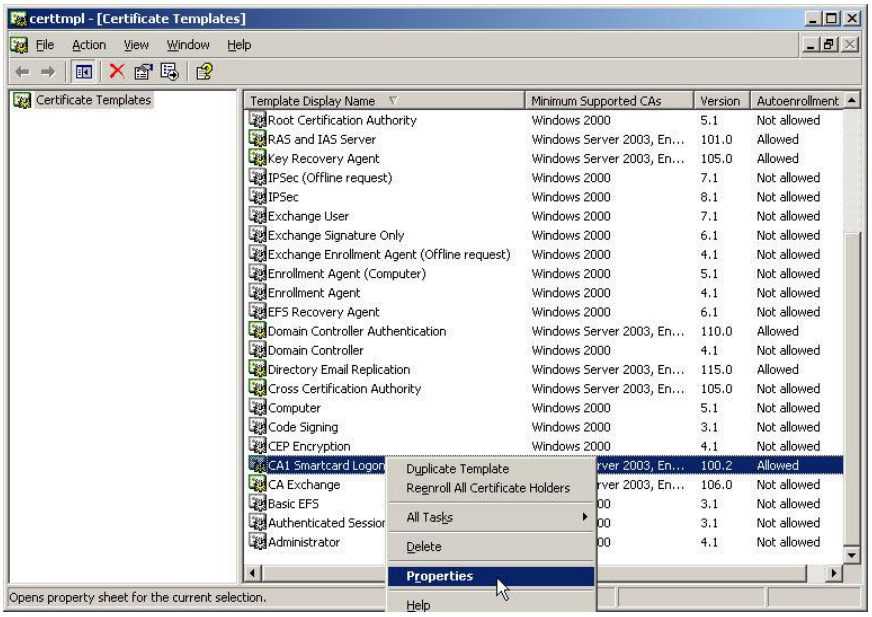
All rights reserved.



6. The new duplicate template will appear in the right-hand details pane of the **Certificate Templates** interface with its new name. Repeat the template duplication procedures for all other templates that will be managed by the CA Administrator for the local CA.

To set permissions and ownership on the duplicate certificate templates:

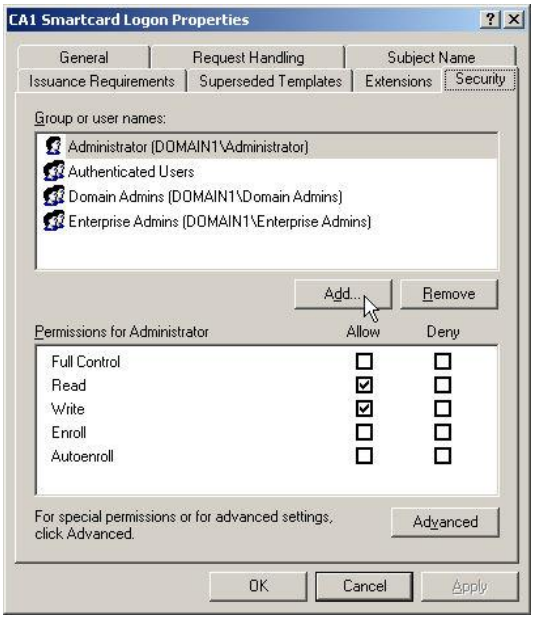
1. In the details pane of the **Certificate Templates** interface, right-click on a certificate template and select **Properties**.



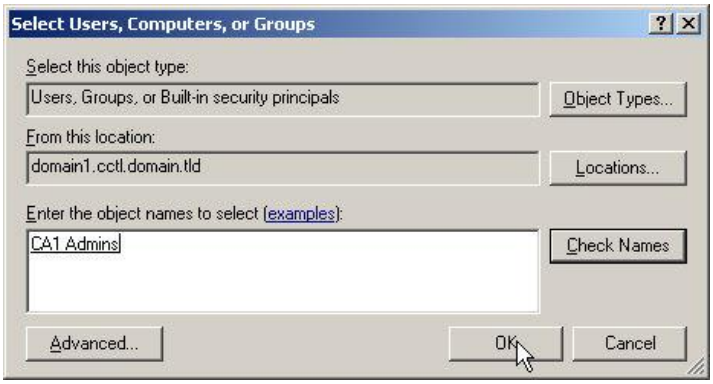
2. The **Properties** interface for the certificate template will appear. Select the **Security** tab to bring it to the foreground then click the **Add** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



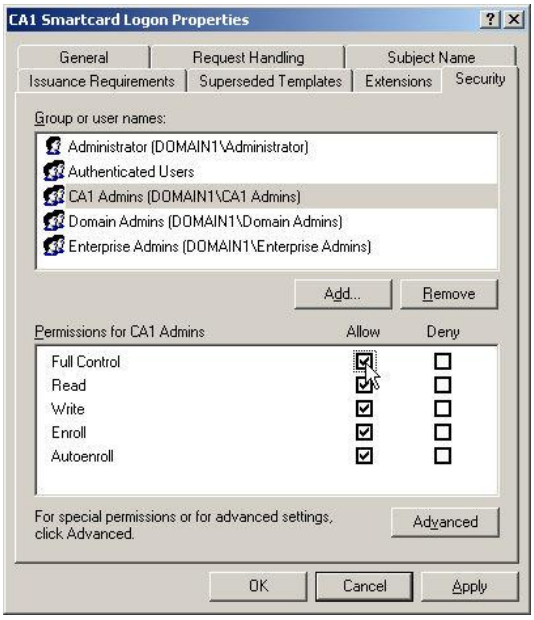
3. The **Select Users, Computers, or Groups** interface will appear. Enter the name of the global group account that is designated for the CA Administrator role. If necessary, click the **Check Names** button to verify that the account exists. Click **OK**.



4. The account will appear in the **Group or user names** box. Highlight the account by selecting it. In the **Permissions for <user name>** window, check the **Allow** box for the **Full Control** permission. The remaining permission boxes will be automatically checked.

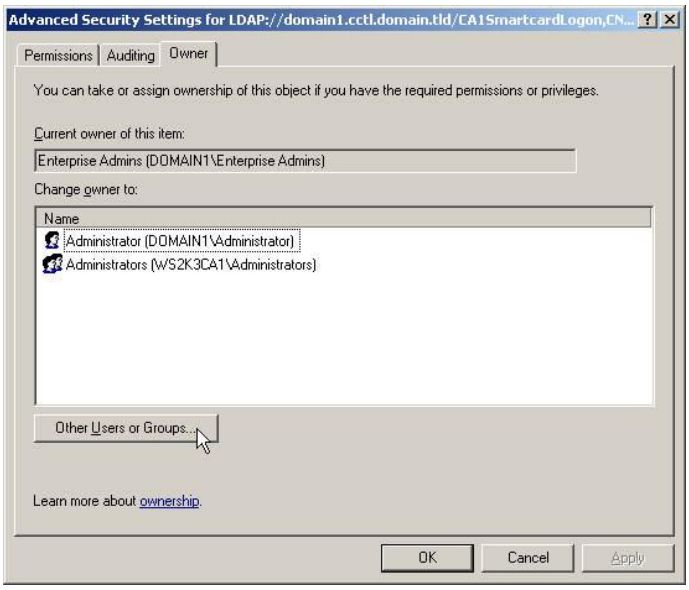
Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. Remove **Write** access to the template for the Administrator, Domain Admins and Enterprise Admins accounts by selecting each account and unchecking the **Allow** box for the **Write** permission.

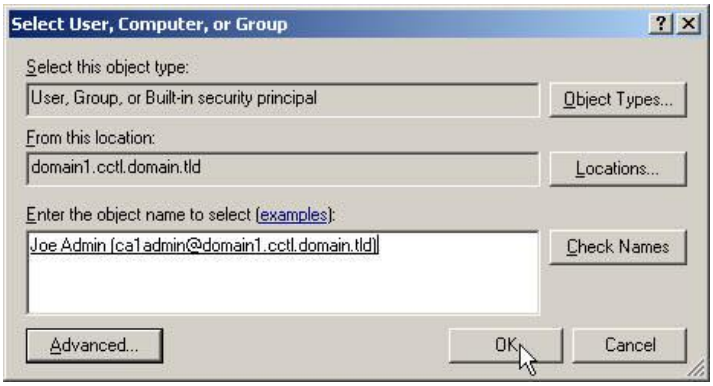
6. Click the **Advanced** button on the **Properties** interface. The **Advanced Security Settings** interface for the certificate template will appear. Select the **Owner** tab to bring it to the foreground.



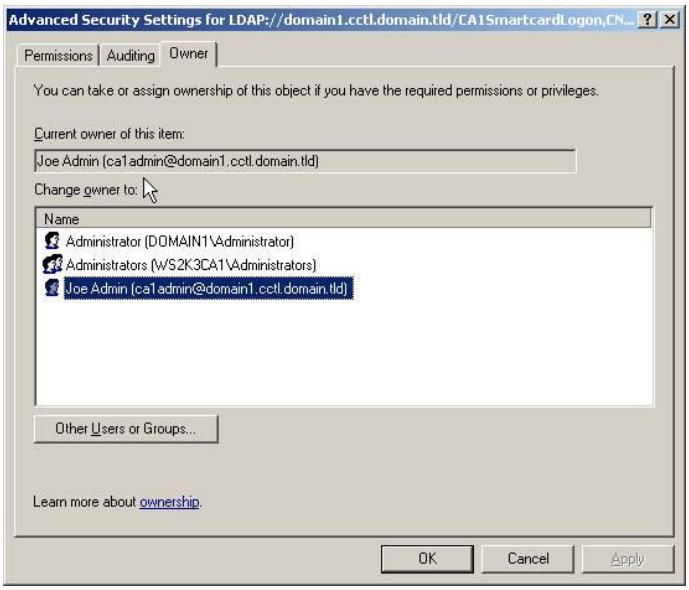
7. Click on the **Other Users or Groups** button. The **Select Users, Computers, or Groups** interface will appear. Enter the name of the "user" account that is designated for the CA Administrator role. If necessary, click the **Check Names** button to verify that the account exists. Click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



8. The account will appear in the **Change owner to** dialog box. Select the account assigned to the CA Administrator role from the **Change owner to** dialog box and click the **Apply** button. The account name will appear in the **Current owner of this item** dialog box.



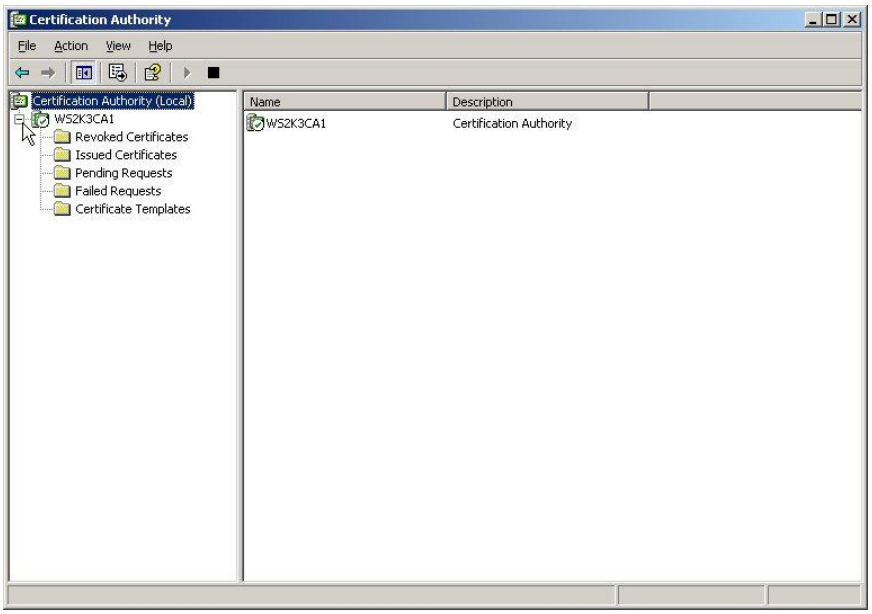
9. Click **OK** to close the **Advanced Security Settings** interface for the certificate template.
10. Click **OK** on the **Properties** interface for the certificate template.
11. Repeat steps 1 through 9 for every remaining certificate template that will be managed from this CA. When finished, exit the **Certificate Templates** interface.

After all duplicate templates required for the current CA are created, they can be added to the CA for issuance. To include a certificate template in the list of certificates available for issuance by the CA, do the following:

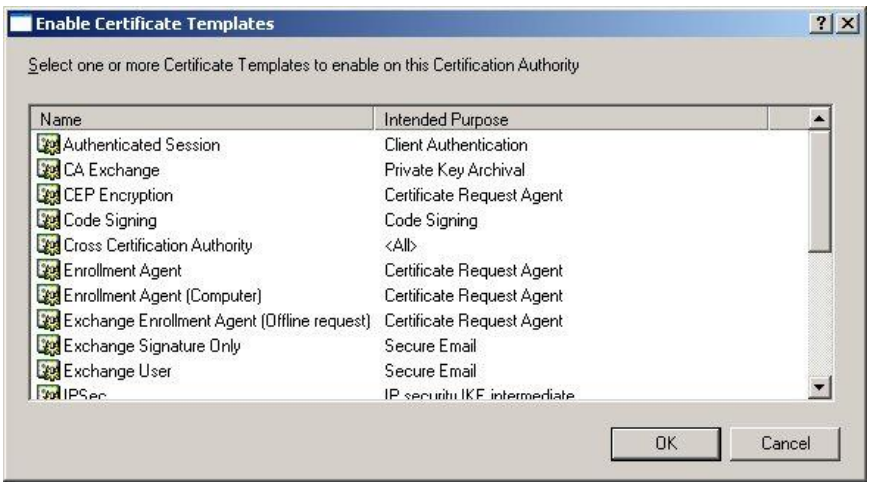
1. Log on to the computer as the CA Administrator.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node to view the **Certificate Templates** folder.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

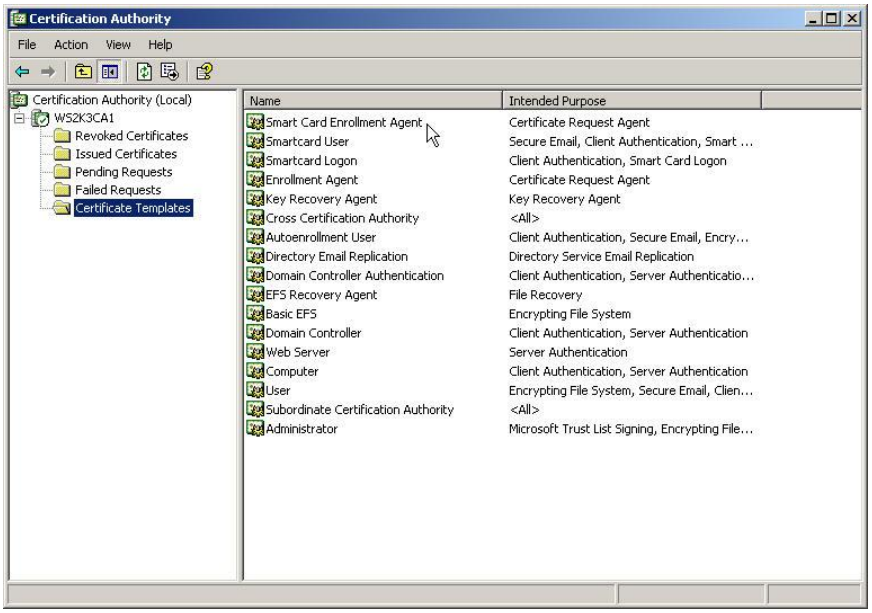


4. Right-click the **Certificate Templates** folder, select **New**, then select **Certificate Template to Issue**.
5. The **Enable Certificate Templates** interface will appear.



6. Select the template to add for issuance and click the **OK** button.
7. Select the **Certificate Templates** folder in the **Certification Authority** interface to verify that the added template appears in the list of templates in the right-hand details pane.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



Role Separation

Role separation enforces the separation of the CA management roles that are defined within the **Certification Authority** interface for role-based administration. Without enabling role separation, a single user can be assigned multiple CA management roles. When enabled, role separation prevents a user with more than one CA role from performing any CA administrative operation. If a user is assigned to more than one role, while role separation is enabled, and attempts to perform a CA administrative operation the action will be denied and the following error message appears:

Enable Role Separation

Before enabling role separation, make certain that no user is assigned to more than one role. If a user is assigned to more than one role and role separation is enabled, then the user will not be permitted to perform any activity for the Certificate Services service.

1. Log on as a member of the local Administrators group.
2. Open a **Command Prompt** window. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**.
3. At the command line type the following command string and hit the Enter key:

   certutil -setreg ca\RoleSeparationEnabled 1
4. A message will be displayed to indicate that the command was completed successfully.
5. Next, Certificate Services must be stopped and restarted in order to load the new Registry entry and enable role separation. At the command line type the following command string and hit the Enter key:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

net stop certsvc

6. The following messages will be displayed indicating the Certificate Services has been stopped:

   The Certificate Services service is stopping.

   The Certificate Services service was stopped successfully.

7. Now, restart the service. At the command line type the following command string and hit the Enter key:

   net start certsvc

8. The following messages will be displayed indicating the Certificate Services has been restarted:

   The Certificate Services service is starting.

   The Certificate Services service was started successfully.

9. Role separation is now enabled. Close the **Command Prompt** window.

Allow the CA Administrator to Set CA Audit Event Categories

In the Evaluated Configuration, only the CA Administrator role is required to set CA audit requirements, while only the CA Auditor is allowed to view and manage the audit logs for the CA. To enforce this specific role separation:

1. Log on as a member of the local Administrators group.
2. Open a **Command Prompt** window. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**.
3. At the command line type the following command string and hit the Enter key:

   certutil -setreg ca\InterfaceFlags +IF_ENABLEADMINASAUDITOR

4. The output should appear as shown below.

```
Old Value:
  InterfaceFlags REG_DWORD = 40 (64)
    IF_NOREMOTEICERTADMINBACKUP -- 40 (64)

New Value:
  InterfaceFlags REG_DWORD = 1040 (4160)
    IF_NOREMOTEICERTADMINBACKUP -- 40 (64)
    IF_ENABLEADMINASAUDITOR -- 1000 (4096)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

5. Next, Certificate Services must be stopped and restarted in order to load the new Registry entry and enable role separation. At the command line type the following command string and hit the Enter key:

   net stop certsvc

6. Now, restart the service. At the command line type the following command string and hit the Enter key:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

net start certsvc

7. The CA Administrator will now be able to set CA specific audit event categories, while the CA Auditor will only be allowed to view and manage the local **Security Events** log for the CA to monitor CA audit events.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Secure Configuration of the Certificate Server

A key aspect of securing the Windows Server 2003 Certificate Server is to first securely configure the host operating system by following the guidance provided in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* for the Common Criteria Evaluated Configuration.

In addition to the protection provided by a securely configured host operating system, the Windows Server 2003 Certificate Server requires the implementation of additional configuration settings that are specific to the protection and secure administration of the Certificate Services.

CA Audit Configuration

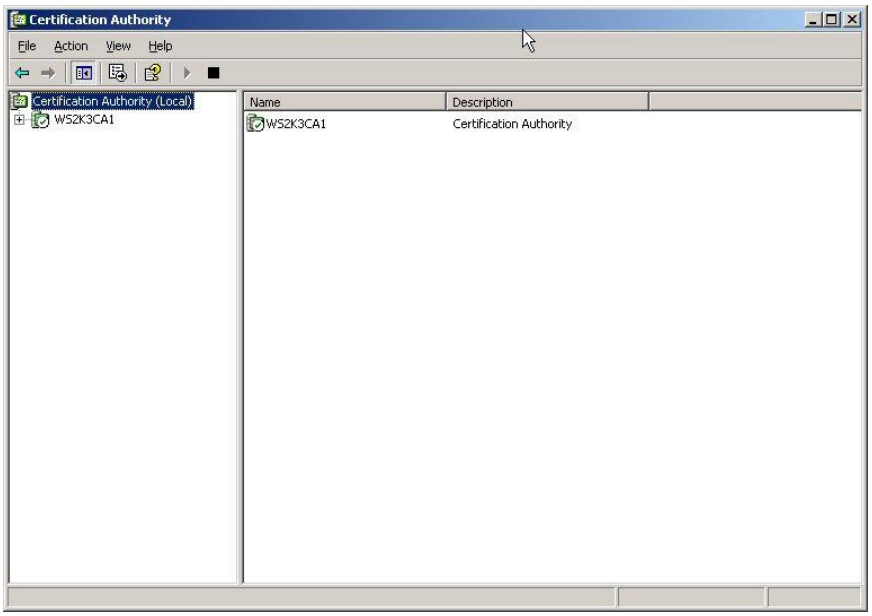
In order to log CA related audit events, it is necessary to first enable system object access auditing on the Windows Server 2003 host. Enabling the **Audit object access** security policy setting to support the configuration of CA Auditing functions is accomplished during the security configuration of the operating system in accordance with the guidelines provided in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* for the Common Criteria Evaluated Configuration.

To enable the ability to log additional security events specific to the management and function of the CA within the operating system's **Security** log, the CA Auditor must select the groups of events to audit from the CA's **Properties** interface.

Note: The setting of selectable CA audit categories is optional, but highly recommended.

Configuration of CA Audit Parameters

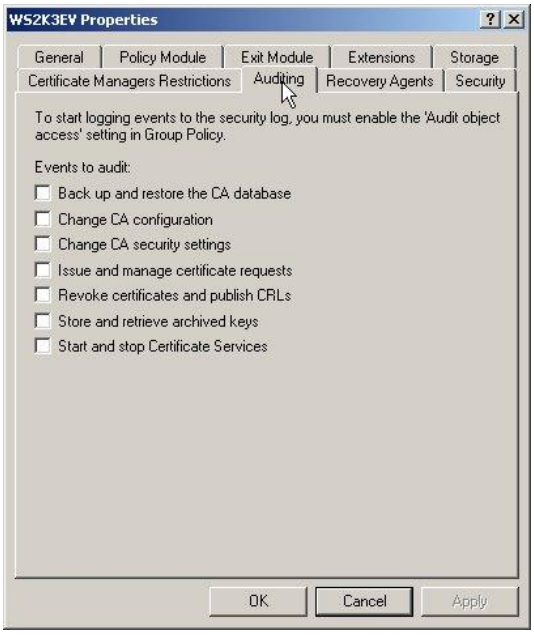
1. Log on to the server hosting the CA as an authorized CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.



3. In the console tree, right-click the CA node, point to **All Tasks**, and select **Properties**. The Certificate Authority's **Properties** interface will appear.
4. Select the **Auditing** tab to display the auditable event groups.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. Select the event group to be audited by checking the box next to each event group listed under **Events to audit**. Table A-5 shows the event groups that can be selected for auditing:

Table A-5 Auditable CA Event Groups for the Evaluated Configuration

CA Audit Group	Description
Back Up and Restore the CA Database	By enabling auditing on this group, successful or failed attempts to back up the CA database will be logged to the system Security log. In addition, the CA service will detect on restart that the CA database has been restored. The restore events are logged to the system Security log.
Change CA Configuration	By enabling auditing on this group, successful or failed attempts to change CA configuration will be logged to the system Security log. This includes the following operations: ▪ Add/Remove Templates to the CA ▪ Configure the CRL Publication Schedule ▪ Modify Request Disposition for the Policy Module ▪ Modify Publish Cert Flags for the Exit Module ▪ Configure CRL Distribution Points (CDP) ▪ Configure Authority Information Access (AIA) ▪ Change the Policy Module ▪ Change the Exit Module ▪ Configure Key Archival and Recovery (KAR)

Copyright © 2008 Microsoft Corporation.
All rights reserved.

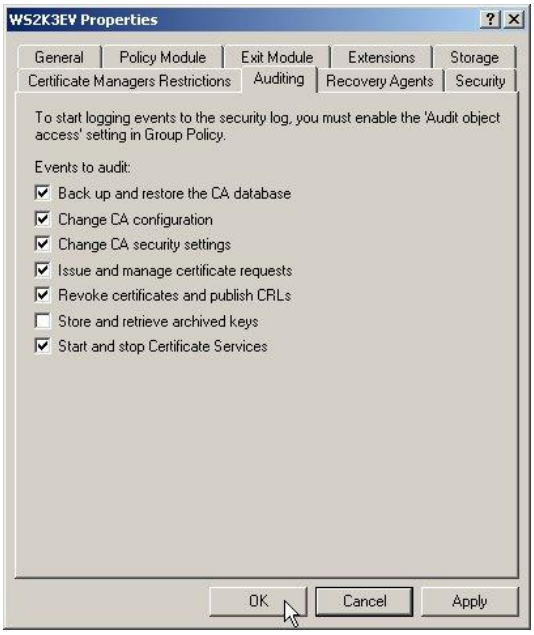
CA Audit Group	Description
Change CA Security Settings	By enabling auditing for this group, successful or failed attempts to change CA security settings will be logged to the system Security log. This includes the following operations: ▪ Configure CA Roles for Role-Based Administration of the CA ▪ Configure Restrictions on Certificate Managers ▪ Configure CA Auditing
Issue and Manage Certificate Requests	By enabling auditing for this group, successful or failed attempts to issue and manage certificate requests will be logged to the system Security log. This includes the following operations: ▪ Incoming Certificate Requests ▪ Certificate Issuance ▪ Certificate Import ▪ Deletion of Rows in the CA Database
Revoke Certificates and Publish CRLs	By enabling auditing for this group, successful or failed attempts to revoke certificates and publish CRLs will be logged to the system Security log. This includes the following operations: ▪ Certificate Revocation ▪ CRL Publication
Start and Stop Certificate Services	By enabling auditing for this group, successful or failed attempts to start and stop Certificate Services will be logged to the system Security log. This includes the following operations: ▪ Starting Certificate Services ▪ Stopping Certificate Services

Note: Details on the specific security events that will be generated by selecting each of the audit groups can be found in Appendix B.

6. When the **Start and stop Certificate Services** box is checked, a message will appear stating that when start and stop events are audited, the time that it will take to stop and start the Certificate Service will increase due to the creation of a cryptographic hash value of the database. Click **OK**.

7. Click **OK** in the **Properties** interface when finished and close the **Certification Authority** interface.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



System Services

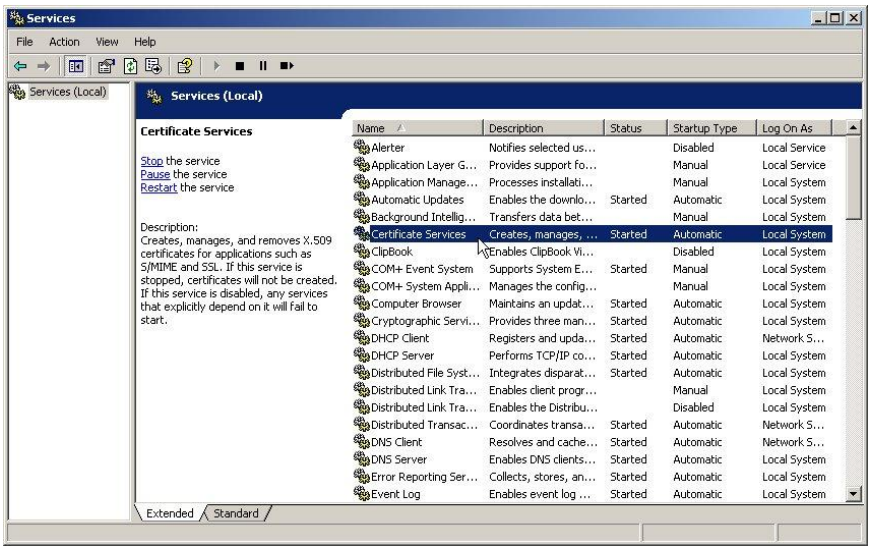
The Certificate Services is part of the core operating system of Windows Server 2003 that enables an organization to act as its own CA. This service is required for Windows Server 2003 Certificate Servers to function properly. The service is used to issue and manage digital certificates for applications, such as Secure/Multipurpose Internet Mail Extensions (S/MIME), SSL, Encrypting File System (EFS), Internet Protocol Security (IPSec), and smart card log on.

Disabling Certificate Services causes certificate requests to not be accepted, and CRLs and delta CRLs will also not be published. Stopping the service long enough will cause CRLs to expire and the validation process for existing certificates to fail. For these reasons, the startup setting for Certificate Services must be configured to **Automatic**. Verify that Certificate Services is configured to startup automatically as follows:

1. Log on with an account that has administrative privileges for the host operating system.
2. Click **Start**, point to **Administrative Tools**, and select **Services**. The **Services** interface will appear. In the details pane, find **Certificate Services** and verify that its **Startup Type** is set to **Automatic**.

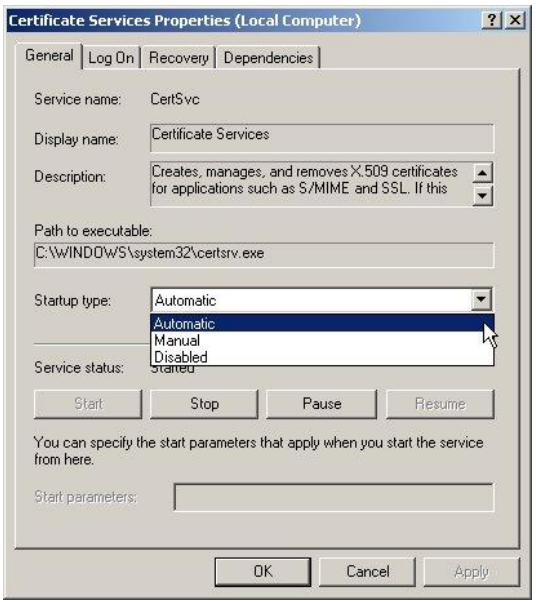
Copyright © 2008 Microsoft Corporation.

All rights reserved.



3. If the service is not set to start up automatically, right-click on **Certificate Services** in the details pane and select **Properties**. The **Certificate Service Properties** interface will appear.

4. Within the **General** tab of the interface, use the **Startup type** drop-down menu to select **Automatic**.



5. If the **Service status** is **Stopped**, click the **Start** button to start the service.

6. Click **OK** to close the **Certificate Service Properties** interface.

Disable Unnecessary System Services

Any service or application is a potential point of attack and, therefore, any unneeded services should be disabled on the Windows Server 2003 Certificate Server host. The Windows Server 2003 host running the Certificate Server should be dedicated solely to function as a Certificate Authority. Therefore, many of the services which are allowed to run in an Evaluated Configuration of Windows Server 2003 are not needed on a Certificate Server host and may be disabled. It is recommended that organizations review the list of system services acceptable for the Windows Server 2003 Evaluated Configuration and disable those which are not necessary for the Certification Authority within the local operating environment.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

To disable unnecessary services:

1. Log on with an account that has administrative privileges for the host operating system.
2. Click **Start**, point to **Administrative Tools**, and select **Services**. The **Services** interface will appear.
3. From the right-hand pane, select a service to disable. Right-click on the selected service and select **Properties**.
4. The **Properties** dialog box for the selected services will appear. From the **Startup type** drop down menu, select **Disabled**.
5. Under **Service status:** click on the **Stop** button.
6. Click the **OK** button.

Securing the Certification Authority's Database and Logs

The *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0* defines the necessary file and folder permissions required to protect the operating system in its Evaluated Configuration. For the Windows Server 2003 Certificate Server host, additional permission settings are required in order to protect the Certificate Authority's database and associated logs.

File and Folder Permissions

The default installation folders are %SystemRoot%\system32\CertLog and %SystemRoot%\system32\CertSrv. Separating the database and logs onto different drives is not a security requirement, but it is recommended for added protection from disk failures and to improve performance by placing these items on separate physical disk devices. If the database and logs are moved from their default location, the appropriate permissions must be applied to the new folders. The required permissions are shown below in Table A-6.

Table A-6 Permissions for CA Database and Logs

Files and Folders	ACL Settings	Inheritance Method
%SystemRoot%\system32\CertLog	**Administrators:** Full Control **Backup Operators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control	Replace
%SystemRoot%\system32\CertSrv	**Administrators:** Full Control **Authenticated Users:** Read and Execute, List Folder Contents, and Read **CREATOR OWNER:** Full Control (Subfolders and files only) **SYSTEM:** Full Control	Replace

Copyright © 2008 Microsoft Corporation.
All rights reserved.

Files and Folders	ACL Settings	Inheritance Method
<Dirve letter>:\CertLog	**Administrators:** Full Control **Backup Operators:** Full Control **CREATOR OWNER:** Full Control **SYSTEM:** Full Control	Replace
<Dirve letter>:\CertSrv	**Administrators:** Full Control **Authenticated Users:** Read and Execute, List Folder Contents, and Read **CREATOR OWNER:** Full Control (Subfolders and files only) **SYSTEM:** Full Control	Replace

Set Permissions on the CA Database and Logs through Windows Explorer

1. Log on with an account that has administrative privileges for the host operating system.
2. Open **Windows Explorer**.
3. Navigate to and select the desired folder (CertLog or CertSrv).
4. Right-click on the file or folder and select **Properties**.
5. In the properties window, select the **Security** tab. Click **Advanced** for more detailed permission settings.
6. Set permissions as necessary. Detailed procedures for setting permissions are provided in the Data Protection subsection of this document.

Note: For the CertSrv folder, allowing inheritable permissions will need to be disabled and the permissions must be set locally.

Auditing of CA Database and Log Access

Because of security and the sensitive nature of CAs, file auditing must be enabled on the Certificate Services folders listed in the preceding table. The audit entries must be configured as shown below in Table A-7:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Table A-7 Auditing of CA Database and Logs

File Path or Registry Path	Audit Type	Audit Setting
%SystemRoot%\system32\CertLog	Fail	Everyone (Full Control)
%SystemRoot%\system32\CertSrv	Success, Fail	Everyone (Modify: Traverse Folder, List Folder, Read Attribute, Read Extended Attribute, Create Files, Create Folders, Write Attributes, Write Extended Attributes, Delete, Read Permissions)
<Dirve letter>:\CertLog	Fail	Everyone (Full Control)
<Dirve letter>:\CertSrv	Success, Fail	Everyone (Modify: Traverse Folder, List Folder, Read Attribute, Read Extended Attribute, Create Files, Create Folders, Write Attributes, Write Extended Attributes, Delete, Read Permissions)

The effect of these settings is to audit any type of failure access (read or modify) from any user and also to audit any successful modification by any user.

Set Auditing on CA Files and Folders through Windows Explorer

1. Log on with an account that has administrative privileges for the host operating system.
2. Open **Windows Explorer**.
3. Navigate to and select the desired folder (CertLog or CertSrv).
4. Right-click on the file or folder and select **Properties**.
5. In the properties window, select the **Security** tab. Click **Advanced** for more detailed permission settings.
6. Select the **Auditing** tab.
7. Click the **Add** button. The **Select Users, Computers, or Groups** dialog box will appear. Enter the name of the account that is to be audited, which is the group **Everyone** as defined in Table 5.3. If necessary, click the **Check Names** button to verify the account. Click **OK**.
8. The **Auditing Entry for <*folder name*>** interface will appear. To audit Full Control for failed access, simply check the **Full Control** box under **Failed** in the **Access** dialog box. To audit Modify rights for success, check the permissions associated with the Modify rights, as defined in Table 5.3, under **Successful** in the **Access** dialog box.

Registry Audit Settings

Table A-8 includes the registry path to the keys and subkeys to audit any changes to the Certificate Server configuration defined in this guide.

Copyright © 2008 Microsoft Corporation.

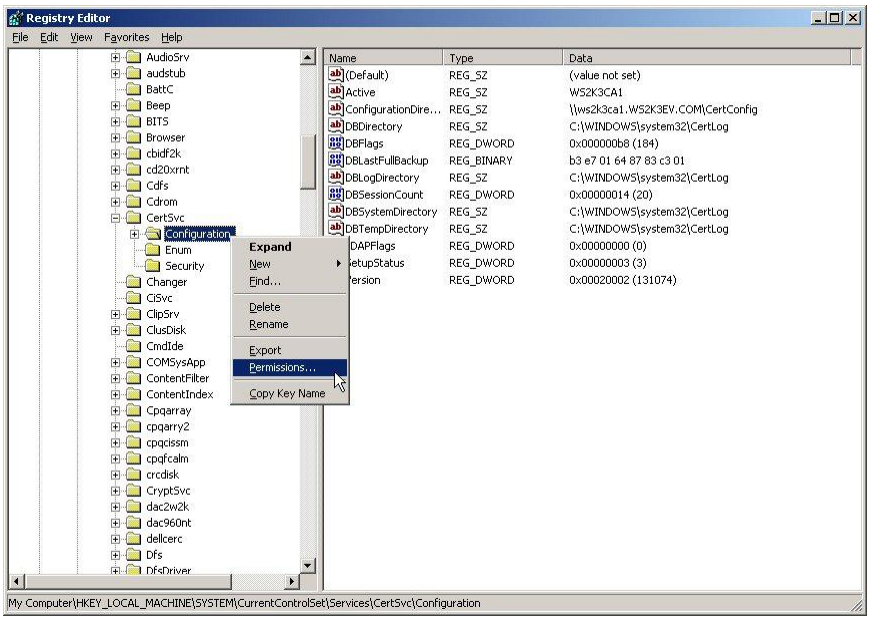
All rights reserved.

Table A-8 Auditing of CA Registry Key

Registry Path	Audit Type	Audit Setting
MACHINE\SYSTEM\CurrentControlSet\Services\Certsvc\Configuration (and all subkeys)	Fail	Everyone (Full Control; <not inherited> Special)
MACHINE\SYSTEM\CurrentControlSet\Services\Certsvc\Configuration (and all subkeys)	Success	Everyone (Special: Set Value, Create Subkey, Create Link, Delete, Write DAC, Write Owner; <not inherited> Special)

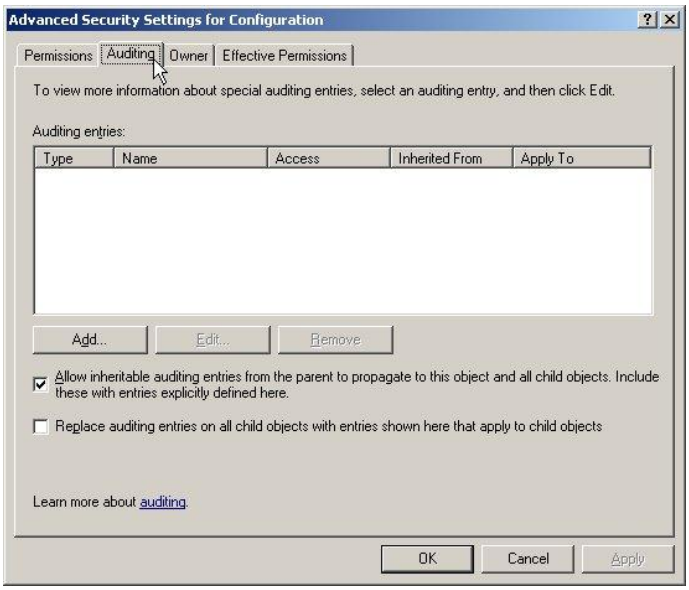
Set Auditing on CA Registry Keys

1. Log on with an account that has administrative privileges for the host operating system.
2. Open the Registry Editor. Click **Start** and select **Run**. Enter **Regedit** in the **Open** dialog box of the **Run** window and click **OK**. The **Registry Editor** interface will appear.
3. Navigate the Registry to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Certsvc\Configuration. Right-click on the **Configuration** subkey and select **Permissions**.

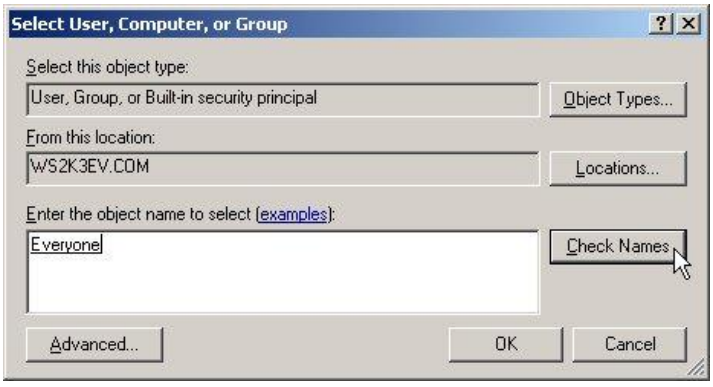


4. The **Permissions for Configuration** interface will appear. Click the **Advanced** button. In the **Advanced Security Settings for Configuration** interface, select the **Auditing** tab.

Copyright © 2008 Microsoft Corporation.
All rights reserved.



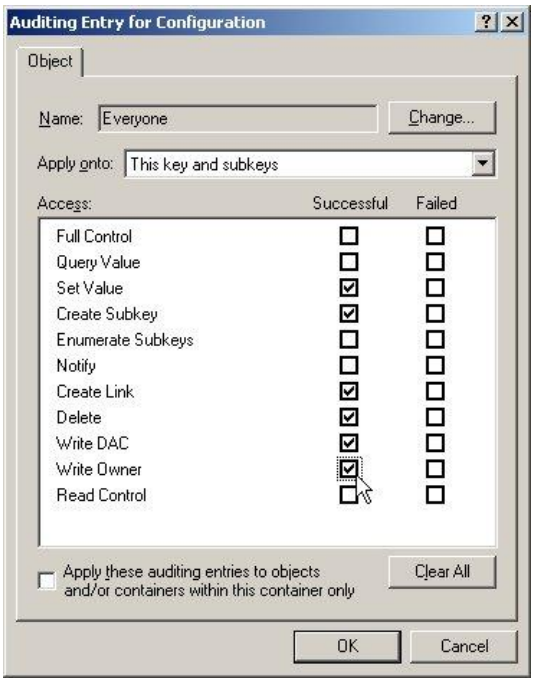
5. Click the **Add** button. In the **Select User, Computer, or Group** interface, enter the name of the account to be audited (the group **Everyone**). Note that it may be necessary to log into the Domain with Domain Admin rights if the account that is to be entered is a domain member. If necessary, find and set the location by using the **Locations** button. Click **OK**.

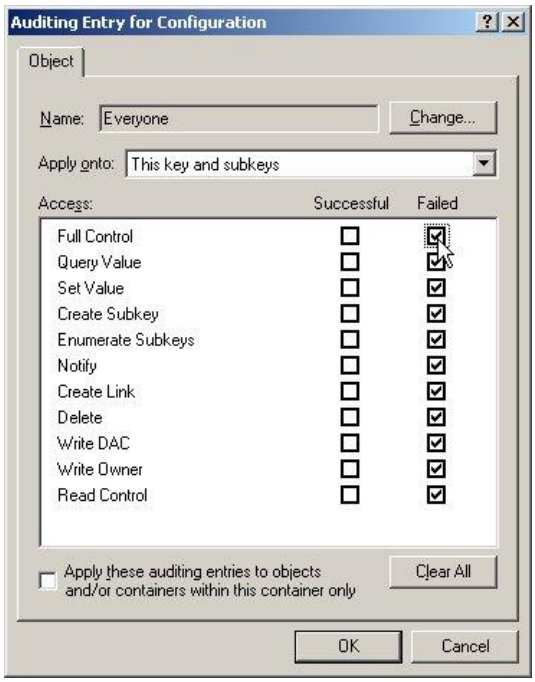


6. In the **Auditing Entry for Configuration** interface, set the audit requirements as defined in Table 5.4. Set one entry for Success auditing and one entry for Failure auditing. For example, for the group **Everyone** there will be one auditing entry for Successful event auditing and then a new setting is created for Failure event auditing.

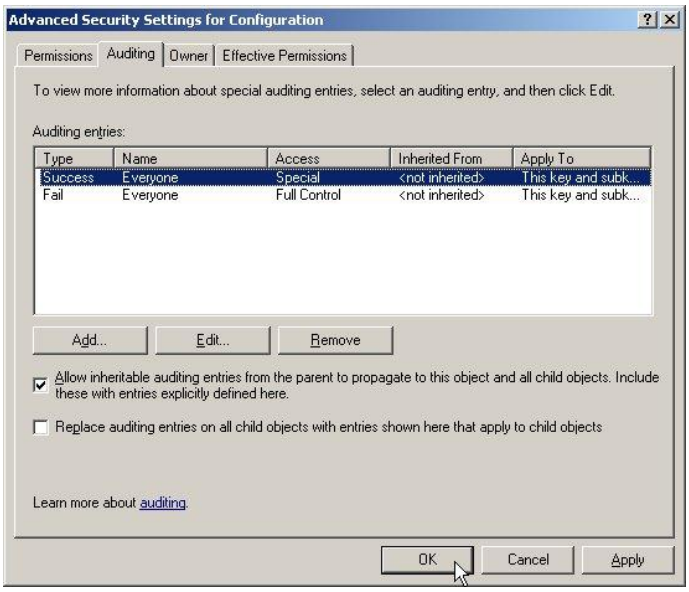
Copyright © 2008 Microsoft Corporation.

All rights reserved.





7. Additional details on setting Registry audit System Access Control Lists (SACLs) are available in the Configuring Audit Policies subsection of this document.



Copyright © 2008 Microsoft Corporation.
All rights reserved.

Appendix B - Windows Server 2003 Certificate Server Administrator's Guide

This Appendix provides and overview of the Windows Server 2003 Certificate Server security functions as well as procedures for administering the Certificate Server in a secure manner. This Appendix does NOT give instruction on how to install and configure the Windows Server 2003 Certificate Server to be in conformance to reside within the TOE. Such instruction is provided in Appendix A. Within this appendix, TOE references pertain to the Windows Server 2003/XP Professional Evaluated Configuration, Version 3.0 TOE.

Audience Assumptions

This document assumes that individuals assigned to the authorized administrative roles defined for the Windows Server 2003 Certificate Server are familiar with the security features of the Windows Server 2003 Certificate Server product and Windows Server 2003 operating system. To administer a Windows Server 2003 Certificate Server, one should also be familiar with relevant product documentation such as the Microsoft Windows Server 2003 Resource and Deployment Kits.

Public Key Infrastructure Concepts

To understand and make effective use of the information provided in this document, system administrators and personnel assigned to authorized Certification Authority (CA) management roles must have a good conceptual understating of PKI, how it is currently being implemented within their organization, or how it must be designed and implemented to best support the specific operational requirements of the organization. Detailed tutorial information on PKI planning and implementation is beyond the scope of this document. However, it is recommended that CA system administrators and personnel assigned to CA management roles become familiar with the information provided in the references below, or other equivalent PKI information, as a prerequisite to administering and maintaining the Windows Server 2003 Certificate Server.

Online PKI Planning Resources

- Designing a Public Key Infrastructure
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b.mspx
- Planning a Microsoft Windows Public Key Infrastructure Using Microsoft Windows Server 2003 (an online presentation)
  http://www.microsoft.com/seminar/shared/asp/view.asp?url=/seminar/en/20030424vcon43/manifest.xml
- Build Guide 2 - Implementing the Public Key Infrastructure
  http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/BGCH07.mspx
- Public Key Infrastructure
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/32aacfe8-83af-4676-a45c-75483545a978.mspx

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Additional PKI Book Resources for Planning

The following books provide detailed information about certificates, certification authorities, public key encryption, and public key infrastructure (PKI).

- Austin, Thomas, PKI: A Wiley Tech Brief. John Wiley & Sons, December 2000.
- Feghhi, Jalal and Jalil Feghhi, Secure Networking with Windows 2000 and Trust Services. Addison-Wesley Pub Co., February 2001.
- Housley, R.P., and T. Polk. 2001. Planning for PKI. New York, New York: John Wiley & Sons, Inc.
- Howard, Michael, Designing Secure Web-Based Applications for Microsoft Windows 2000. Microsoft Press, August 2000.
- Kaufman, C., Perlman, R., and M. Speciner. 1995. Network Security: Private Communication in a Public World. Upper Saddle River, New Jersey: Prentice-Hall Inc.
- Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, December 1995.

Overview of Security Functions

This subsection provides an overview of the security functions of the Windows Server 2003 Certificate Server.

- **Identification and Authentication** – The Certificate Server, in conjunction with the IT Environment, ensures that users are identified and authenticated before they can access any other security-relevant services. All local or remote communications with the Certificate Server are completed over Kerberos-enabled secure Distributed Component Object Model (DCOM) channels that require the client to be known to the IT Environment prior to allowing the communication channel to be established.
- **Access Control** – The Certificate Server enforces user roles and access control whenever users access services provided by the Certificate Server. To enforce its security policy, the Certificate Server enforces roles through the use of Operating System policies and Access Control Lists (ACL) managed by the Certificate Manager. IT Environment administrators are responsible for assigning IT Environment policies for users and CA Administrators are responsible for defining the ACLs maintained by the Certificate Server. Access Control is primarily enforced by ensuring a user is mapped to a role before any security-relevant operation is performed.
- **Security Management** – The Certificate Server uses access control functions to control the actions of administrative staff. In order to accomplish this, predefined access control lists are assigned to the applicable services.
- **Security Audit** – By using the auditing infrastructure of the IT Environment, the Certificate Server has the capability to generate audits for security-relevant events associated with the services that it provides. Certificate issuance and management related audit records (which include the responsible user identity, date, time, and other details) are generated when their associated audit events occur inside the Certificate Server. The Certificate Server tracks actions related to a certificate (request pending, request denial, creation, publication and revocation), changes to user's roles and access, certificate database backup and restore operations, and modifications to the Certificate Server configuration. After receiving the audit records from the Certificate Server, the IT Environment audit infrastructure protects them, together with other IT Environment security-relevant audit records, in its in-memory audit queue. Concurrently, the IT Environment empties its audit queue by writing the queue elements to a persistent audit log file that it has opened executively for its own access only during system boot.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Backup and Recovery** – The Certificate Server has a backup/restore service for its certificate database that can be used by an authorized user to save a snapshot of its configuration as represented by the certificate database and then restore that configuration at a later date.
- **Remote Certificate Request Data Entry and Certificate Status Export** – The Certificate Server processes certificate requests formatted according to the following standards:
  - Public Key Cryptography Standard (PKCS) #7 (Cryptographic Message Syntax Standard),
  - PKCS #10 (Certification Request Syntax Standard),
  - Request for Comment (RFC) 2797 CMC (Certificate Management Messages over Cryptographic Message Syntax).
- **Key Management** – The Certificate Server can use a hardware cryptographic module for various key management functions. In particular, security critical keys and other information are protected by either encrypting or storing them within a hardware cryptographic module. Within the TOE, security critical keys and other information do not leave the hardware cryptographic module in clear text format. Digital signatures are used when appropriate to ensure the integrity of key management related information.
- **Certificate Management** – The Certificate Server includes a number of certificate management functions. In particular, CA administrators can control, limit, or mandate values in certificates and CRLs.
- **Certificate Templates for Certificate Profile Management** – Certificate templates define the attributes for certificate types. Authorized users can configure the Certificate Server to issue specific certificate types to authorized users, services and computers. When the Certificate Server creates a certificate, a corresponding certificate template is used to specify its attributes, such as the authorized uses for the certificate, the cryptographic algorithms that are to be used with it, the public key length, and the certificate lifetime. Certificate templates are stored in Active Directory and provide information for each of type of certificate. The Certificate Server queries the Active Directory for the set of templates that it uses for issuing certificates. A number of pre-configured, commonly used certificate templates are available.
- **Qualified Subordination** – Qualified subordination allows cross-certification of CA certificates with constraints based on use and length of certificate path, names allowed in certificate, and policies accepted and thus provides for more granular control of certificate trusts. With qualified subordination an authorized administrator can also include or exclude certificate purposes. For example, qualified subordination might reject Internet Protocol Security (IPSec) usage with a 3rd party certificate but allow secure email with the same certificate even if the certificate's key usage would allow IPSec and secure email.
- **Role Separation** – The Certificate Server enforces the administrative actions for each role to be performed by accounts that have been assigned that specific role. The following roles are defined:
  - CA Administrator
  - Certificate Manager
  - Auditor
  - Backup Operator
- **Support for Auto-Enrollment** – As Active Directory can define the permission for a specific account to enroll to a certificate template, the use of certificate templates in the Certificate Server allows automatic certificate issuing based on the certificate profile information contained in a particular certificate template that a certificate requester has permission to enroll to.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

CA Management Roles and Associated Privileges

Role-based administration features of Windows Server 2003 Certificate Services can be used to organize administrative staff into separate, predefined task-based CA management roles, each with their own set of tasks. Roles are assigned to a user by granting that user the specific security permissions and user rights that are associated with the role. A user who has one type of permission, such as Manage CA permission, may perform specific CA tasks that a user with another type of permission, such as Issue and Manage Certificates permission, may not perform.

Role-based administration supports assignment of roles to users and groups. To assign a CA management role to a user or group, corresponding security permissions, group memberships, or user rights that define each role must be assigned to the selected accounts in order to grant them the explicit capabilities assigned to each role. Table B-1 describes the CA management roles relevant to Windows Server 2003 Certificate Server role-based administration.

Table B-1 CA Management Roles

Roles	Required CA Security Permissions / User Rights / Group Membership	Description
CA Administrator	**CA Security Permissions:** (Applied through the CA Properties interface) Allow **Manage CA** permission.	Configures and maintains the CA. This is a CA management role defined through CA specific security permissions.
Certificate Manager (Officer)	**CA Security Permissions:** (Applied through the CA Properties interface) Allow **Issue and Manage Certificates** permission.	Approves certificate enrollment and revocation requests. This is a CA management role defined through CA specific security permissions. This role is sometimes referred to as CA Officer.
CA Backup Operator	**Group Membership:** (Default built-in group on CA host) Add to **Backup Operators** group. (provides **Back up file and directories** and **Restore file and directories user** privileges)	Performs CA system backup and recovery. This is a CA management role defined through operating system based user rights.
CA Auditor	**User Rights:** (Local user right on CA host) Grant **Manage auditing and security log** privilege.	Configure, view, and maintain audit logs. This is a CA management role defined through operating system based user rights.

Network-level IT Environment

Within the TOE, the Windows Server 2003 Certificate Server is intended to operate in a networked environment in which it supports and is supported by other systems that use Windows Server 2003 and Windows XP Professional operating systems. This section describes the networking environment for which the Certificate Server is intended to be used. Administrative staff should ensure that the network-level IT environment meets these networking conditions regarding the specific systems supported.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Networked Systems Supported by the Certificate Server

Within the TOE, the Windows Server 2003 Certificate Server can provide certificate services to:

- Other Certificate Servers that act as subordinate CAs or peer CAs within the TOE.
- Windows Server 2003 platforms that are not Certificate Servers.
- Windows XP Professional workstations.

Networked Systems Supporting the Certificate Server

Within the TOE, Windows Server 2003 Certificate Server can receive services from:

- Other Certificate Authorities that act as root or parent CA's.
- Other Windows Server 2003 Certificate Servers that act as peer CAs.
- Windows Server 2003 Domain Controllers in support of an enterprise CA which authenticate users, store certificate templates, and publish certificates and CRLs.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Administering Windows Server 2003 Certificate Server Security

This section describes effective security practices for administering the Certificate Server in a secure manner. Specific topics covered in this section include the following:

- Certificate Server Security Management Interfaces
- Security Functions
- Security-relevant Events

Certificate Server Security Management Interfaces

This subsection provides a brief description of the security management interfaces used to administer the Windows Server 2003 Certificate Server.

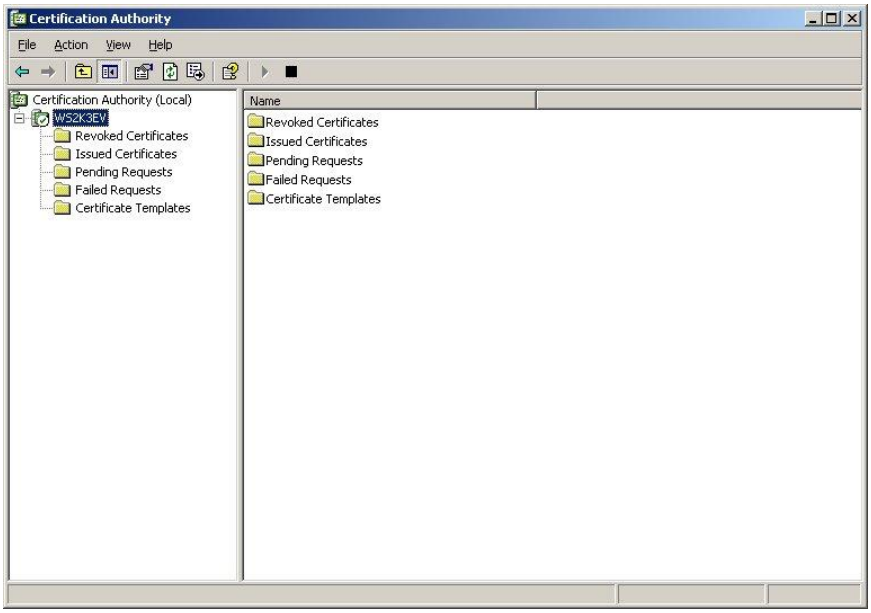
Microsoft Management Consoles

The following Microsoft Management Console (MMC) snap-ins provide the interfaces used to administer the Certificate Server.

- Certification Authority MMC Snap-in
- Certificates MMC Snap-in
- Certificate Templates MMC Snap-in.

Certification Authority MMC Snap-in

The Certification Authority Snap-in authorizes CA management roles to access customizable services for issuing and managing certificates that are used in software security systems that employ public key technology. A CA receives certificate requests, verifies the information in the request and the identity of the requester, issues certificates, revokes certificates, and publishes a CRL.

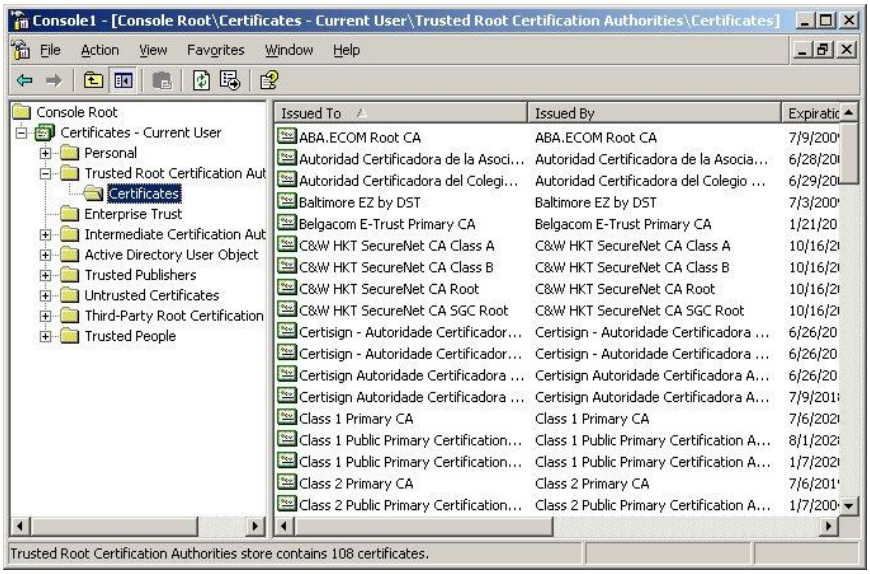


Copyright © 2008 Microsoft Corporation.

All rights reserved.

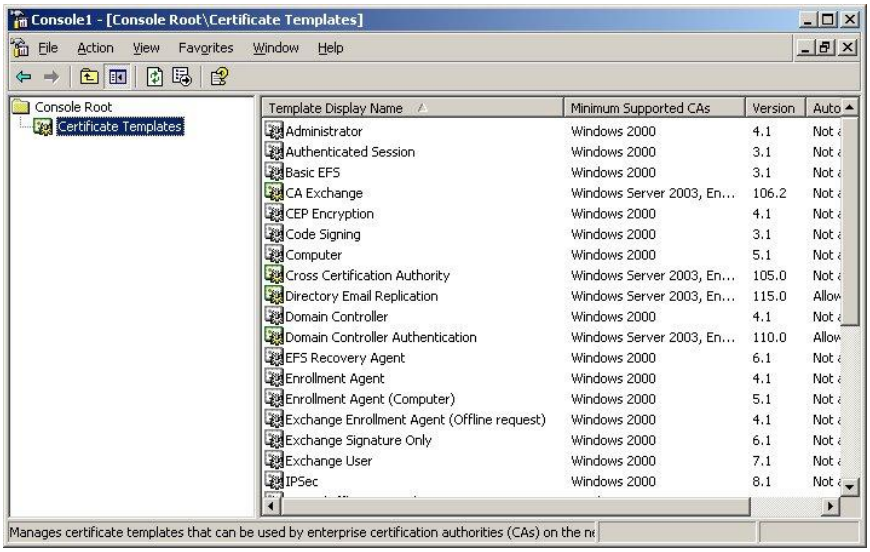
Certificates MMC Snap-in

The Certificates Snap-in allows the user to manage existing certificates and request new certificates from a CA.



Certificate Templates MMC Snap-in

Certificate templates are available for enterprise CAs and provide the default contents of all certificates that can be requested from an enterprise CA. The Certificate Templates Snap-in is used to manage these certificate templates.



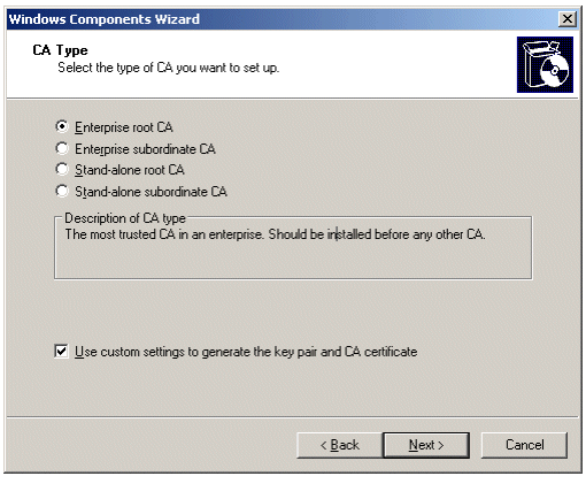
Configuration Wizards

The **Windows Components Wizard** is used to install a Certificate Server. To install an enterprise root or subordinate CA, an authorized administrator must be logged onto the domain with Enterprise

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Administrator privileges. Otherwise, the **Enterprise root CA** and **Enterprise subordinate CA** types will not be selectable via the wizard (they will be grayed out).



Command-line Tools

The use of three command line tools is described within this document.

- **certutil.exe**. In general, the **CertUtil** command may be used to dump and display CA configuration information, configure Certificate Services, configure enforcement of CA role separation, back up and restore CA components, and create cryptographic hash files.
- **net.exe**. This tool is primarily used to start and stop certificate services from a command line.
- **certreq.exe**. This tool is primarily used to generate, submit, and retrieve certificate requests files and certificates.

Security Functions

This subsection identifies all the security functions available to administrative staff and needed to operate the Windows Server 2003 Certificate Server securely. Administrative tasks fall into two categories– configuration tasks and day-to-day management tasks. Configuration tasks are described in the Appendix A - Windows Server 2003 Certificate Server Security Configuration Guide. Table B-2 provides an overview of the day-to-day management tasks for a CA and the responsible administrative roles.

Table B-2 Overview of Management Tasks

Activity	CA Administrator	Certificate Manager	Auditor	Backup Operator	Local Administrator	Notes
Install CA					X	
Configure policy and exit module	X					

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Activity	CA Administrator	Certificate Manager	Auditor	Backup Operator	Local Administrator	Notes
Stop and start the Certificate Services service	X			X*		*The CA Backup Operator may use the certutil.exe utility with the –shutdown flag to shutdown the CA before restoring the CA database. However, the CA Backup Operator is not allowed to start the CA.
Configure extensions	X					
Configure roles	X					
Renew CA keys and certificates					X	
Define key recovery agents	X					
Configure Certificate Managers restrictions	X					
Delete single row in database	X					
Delete multiple rows in database (bulk deletion)					X	
Enable role separation					X	
Issue and approve certificates		X				
Deny certificates		X				
Revoke certificates		X				
Reactivate certificates placed on hold		X				
Enable, publish, or configure	X					

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Activity	CA Administrator	Certificate Manager	Auditor	Backup Operator	Local Administrator	Notes
CRL schedule						
Configure audit parameters			X			By default, the local Administrator holds the system audit privilege.
Audit logs			X			By default, the local Administrator holds the system audit privilege.
Back up system				X		By default, the local Administrator holds the system backup privilege.
Restore system				X		By default, the local Administrator holds the system restore (backup) privilege.
Read CA database	X	X	X	X	X	By default, the local Administrator holds the system audit and backup privileges.
Read CA configuration information	X	X	X	X	X	By default, the local Administrator holds the system audit and backup privileges.

Notes:

- By default, enrollees are allowed to read CA properties and CRLs, and can request certificates. On an Enterprise CA, a user must also have Read and Enroll permissions on the certificate template to request a certificate.
- CA Administrators, Certificate Managers, the Auditor, and Backup Operators have implicit Read privileges on the CA.
- An Auditor is based on a user that holds the system **Manage auditing and security log** privilege. The local Administrator by default on each machine always holds the system **Manage auditing and security log** privilege. Before role separation is enabled, a separate user must be configured to manage audit for the CA by assigning that user the local system **Manage auditing and security log** privilege.
- A Backup Operator is based on a user that holds the system **Backup files and directories** and **Restore files and directories** privileges.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- It is required to have both CA Administrator and Certificate Manager roles to do bulk deletion, so any person who has both the roles will be able to perform bulk deletion. When role separation is enabled, this feature is not available.

- For issuing failed certificate requests, it is required to have both CA Administrator and Certificate Manager permissions. When role separation is enabled, this feature is not available.

The subsections that follow describe the detailed procedures required to perform the day-to-day management tasks for the four different types of CAs.

Role-Based Certification Authority Management

Role-based administration involves the use of explicitly assigned CA management roles. To assign a CA management role to a user or group, the corresponding security permissions or user rights that define each role must be assigned to the selected accounts in order to grant them the explicit capabilities assigned to a role. Table B-1 describes the CA management roles relevant to the Windows Server 2003 Certificate Server role-based administration. Table B-2 defines the CA relevant management tasks that each role is capable of performing.

Assignment of Certification Authority Management Roles

Detailed procedures for the assignment of CA management roles are provided in Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide. It is important that no single user account ever be assigned to more than one CA management role. This will ensure support for separation of security management responsibilities for the CA. CA role separation is enforced within the TOE, ensuring that users will not be allowed to perform any CA administrative task if they are assigned to more than one role.

To assign a user to a CA management role, simply add the user to the pre-configured group account designated for that role, as recommended in Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide. Procedures for creating and managing user accounts and group memberships are provided in the Creating and Maintaining User and Group Accounts subsection of this document.

Removing Role Assignments

To remove a user's CA management rights, simply remove the user account from the pre-configured group account for that role. Prior to removing a user's CA management rights, ensure that the right has been granted to another designated user account assigned to take over that CA management role.

Administering a Certification Authority

There are a number of tasks performed by CA management roles as a part of normal service operation. These include the following:

- Starting and stopping the service;
- Backing up and restoring the service;
- Configuring CA event auditing;

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- Renewing CA certificates;
- Managing certificate revocation;
- Managing certificate requests;
- Managing certificate profiles;
- CA key management; and
- Changing policy settings on a CA.

Starting and stopping certificate services

To perform several CA administrative tasks, it is necessary to stop and restart certificate services. Once the CA is configured, the service will start by default. The following procedures show how to stop and restart certificate services using either the **Certification Authority** interface or the **net.exe** command line tool.

To stop and start certificate services using the **Certification Authority** interface:

1. Log on using the CA Administrator role.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. In the console tree, right-click the name of the CA, point to **All Tasks**, and click **Stop Service** to stop the service or click **Start Service** to start the service.

To stop and start certificate services using the **net.exe** command line tool:

1. Log on as an authorized administrator.
2. Open a command line interface. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**.
3. Type **net stop certsvc** to stop the service or type **net start certsvc** to start the service.

Certification Authority backup and recovery

Development of recovery procedures to provide periodic backups of Certification Authority information is extremely important to ensure the continued availability of certificate services for an organization. The Windows Server 2003 Certificate Server provides a backup and restoration tool, called the **Certification Authority Backup Wizard,** that can be used to recover from catastrophic system or machine failures that may impact the computer hosting the CA. The CA backup and restoration tool can be used to backup and restore certificates, and the certificates database (the database of issued certificates and the queue of pending requests). Failure to implement backup and recovery procedures means that the organization supported by the CA may be unable to preserve their records of certificate requests and issued certificates, and may lose the ability to revoke issued and previously un-revoked certificates. This section describes backup and restore features available to administrators for this purpose.

The Certification Authority Backup Wizard is used to first create a full backup, and then create incremental backups after the full backup is completed. When restoring the certificates database, it is important to first restore the full backup, and then restore all of the incremental backups in the order that they were created.

Copyright © 2008 Microsoft Corporation.

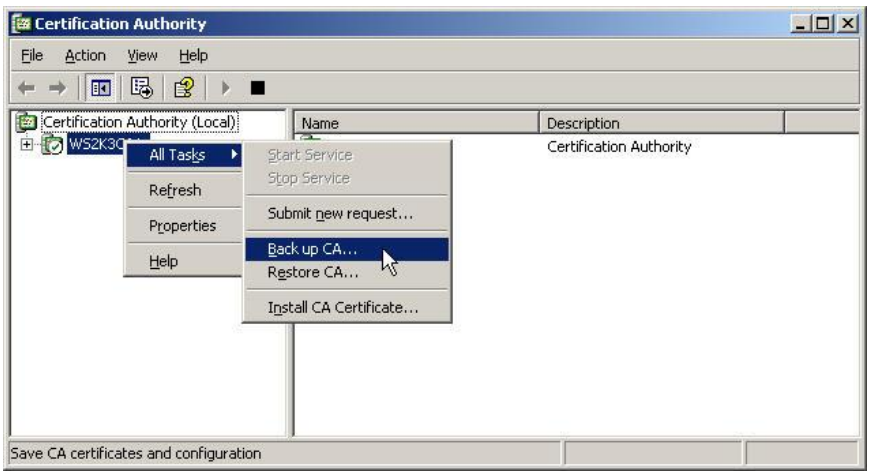
All rights reserved.

Back up the certificate database and certificate database log

Within the TOE, the CA's private key is protected by the Hardware Security Module. Therefore, backup of the CA's private key cannot be accomplished using the **Certification Authority** interface or the **Certutil.exe** command line utility.

To back up the CA's certificate database and certificate database log:

1. Log on to the server as an authorized CA Backup Operator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. In the console tree, right-click the name of the CA, point to **All Tasks**, and select **Back up CA**.

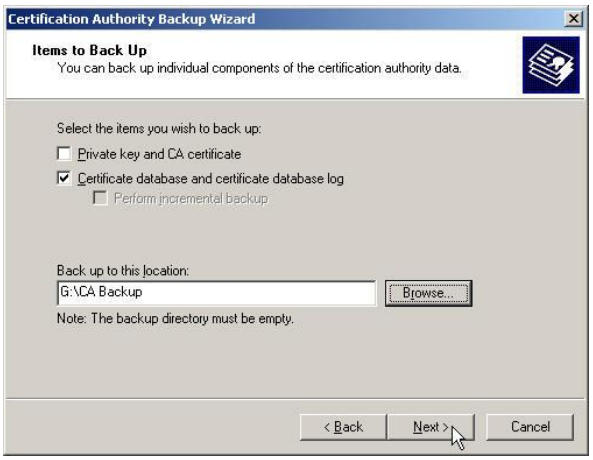


4. On the "**Welcome to the Certification Authority Backup Wizard**" page, read the introductory text, and then click **Next**.

5. On the "**Items to Back Up**" page, click to select the **Certificate database and certificate database log** check box. If a full backup already exists, the **Perform incremental backup** check box will become active. A new backup folder will need to be created for storing the incremental backup files. In the **Back up to this location** box, type a local path to an empty folder. If the folder that is typed in does not already exist, the Wizard will create the folder. Click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



- The **Private key and CA certificate** checkbox is not an option within the TOE because the CA private key is protected by the associated hardware cryptographic module and is not accessible by the **Certification Authority Backup Wizard**. If an attempt is made to backup the private key, the following message will appear:

- If the specified backup location contains a previous backup, a message will appear indicating that the directory is not empty. Specify a new backup location in order to continue.

Note: The user account that is assigned the role of CA Backup Operator will need to have permissions defined for the folders storing the CA backup information. Set permissions on the CA backup folders and all contents to only allow the CA.

6. On the **Completing the Certification Authority Backup Wizard** page, click **Finish**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

7. A progress bar appears that shows the status of the backup job. When the backup job is complete, the **Certification Authority Backup Wizard** closes. If no further CA Backup Operator tasks are required, exit the **Certification Authority** interface and log out of the CA Backup Operator role.

Confirm that the backup file was created by using **Windows Explorer** to navigate to the location supplied in step 5 above. In that folder, there will be folder named DataBase. In the DataBase folder, there will be three files, one each with suffixes .dat, .log, and .edb.

Using **Certutil.exe** to back up the CA database:

1. Log on to the server as an authorized CA Backup Operator.
2. Open a command line interface. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**.
3. Type:

certutil –backupDB <BackupDirectory> keeplog

Value	Description
-backupDB	Specifies a backup of the CA's database.
BackupDirectory	Specifies the path to use to store the backup data.
Keeplog	Ensures all the logs are backed up, preventing them from being truncated.

Create a cryptographic hash of the backup files

It is recommended that all CA backup files be saved to a secured network location or to removable media that is then stored in a physically protected location away from the TOE. A cryptographic hash of the backup files can be made in order to later verify the integrity of the backups prior to their restoration.

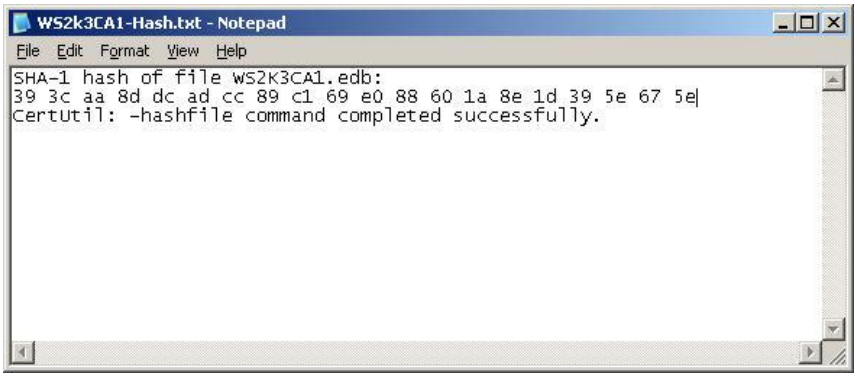
To create a cryptographic hash of the backup files use the certutil.exe using the command string format shown below and save the results to a file.

certutil –hashfile <filename>

For example, if the filename is ***WS2K3CA1.edb*** use the command string shown below to pipe the results to a file called ***WS2K3CA1-Hash.txt***.

Certutil –hashfile WS2K3CA1.edb >WS2K3CA1-Hash.txt

The resulting hash information is stored to a text file:



The hash information should be stored and secured separately from the backup data.

Copyright © 2008 Microsoft Corporation.

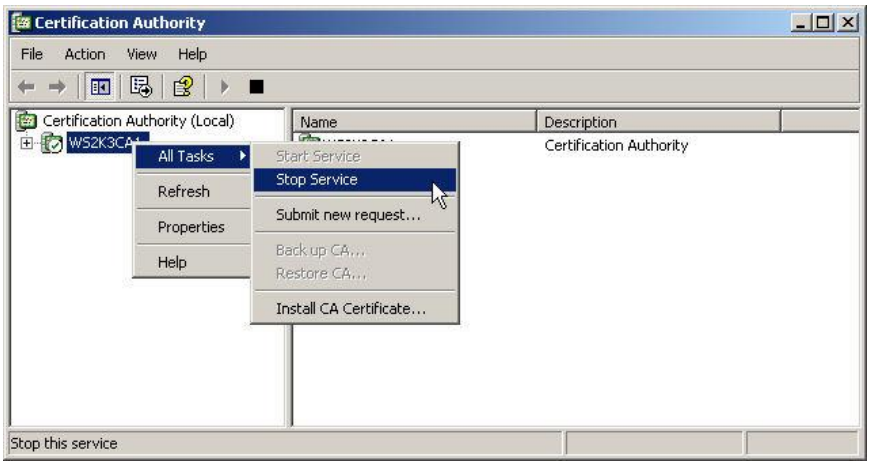
All rights reserved.

Restore the certificate database and certificate database log

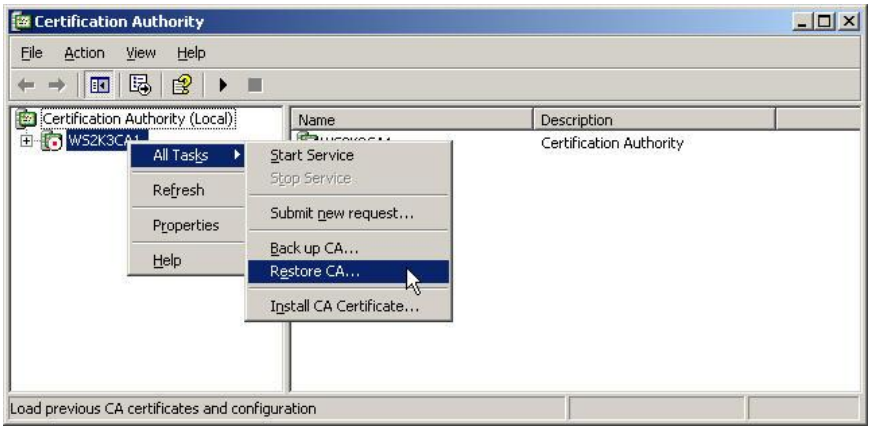
The Certification Authority cannot be restored from a backup if its service is running. Therefore, it will be necessary to stop the CA Server service prior to restoration. Only authorized system administrators and CA administrators are allowed to start and stop the CA service.

To restore the Certification Authority from a backup:

1. Log on to the server as an authorized CA Administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**. The **Certification Authority** interface will appear.
3. Right-click the CA, point to **All Tasks**, and then click **Stop Service**. A **Stopping Certificate Services** progress bar appears. When Certificate Services has been stopped, a red "x" will appear next to the CA icon in the **Certification Authority** interface.



4. Log out of the CA Administrator role.
5. Log on to the server as an authorized CA Backup Operator.
6. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then select **Certification Authority**. The **Certification Authority** interface will appear.
7. Right-click the CA, point to **All Tasks**, and then select **Restore CA**.

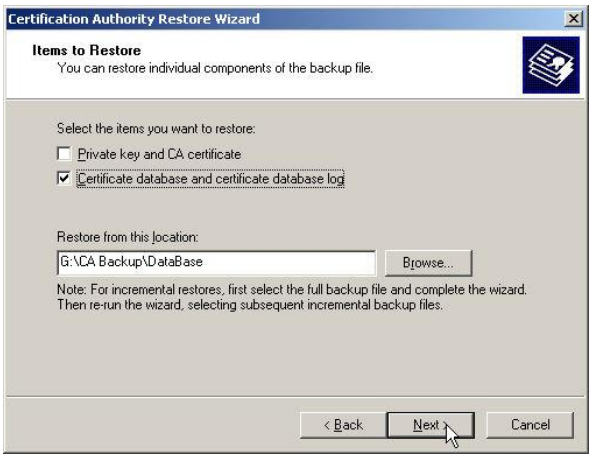


8. On the **Welcome to the Certification Authority Restore Wizard** page, read the introductory text, and then click **Next**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

9. On the **Items to Restore** page, click to select the **Certificate database and certificate database log** check box. In the **Restore from this location** box, type the path to the certificate services backup, or click **Browse** to locate the folder. Click **Next**.



Notes:

To restore the incremental backups, the full backup must first be restored through the **Certification Authority Restore Wizard**. After the full backup restoration is completed, the wizard will need to be executed again to restore the incremental backups.

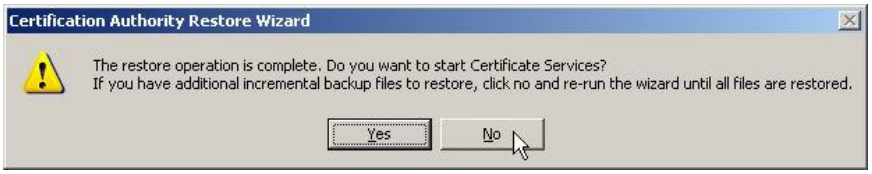
The **Private key and CA certificate** checkbox is not an option within the TOE because the CA private key is protected by the associated hardware cryptographic module and is not backed up by the **Certification Authority Backup Wizard**.

10. On the "**Completing the Certification Authority Restore Wizard**" page, click **Finish**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

11. After the restoration is complete, a **Certification Authority Restore Wizard** interface states that the restoration operating is complete and offers to start certificate services. Since the Backup Operator role is not permitted to start the CA service, click **No**. Also, if incremental backup files are to be restored, click **No** and re-run the wizard until all the incremental backups have been restored.



Note: If the CA Backup Operator attempts to start Certificate Services, the following error message will appear:

12. After all CA restoration procedures are completed, log out of the CA Backup Operator role and log back in as an authorized CA Administrator.
13. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**. The **Certification Authority** interface will appear.
14. Right-click the CA, point to **All Tasks**, and then click **Start Service**. A "**Starting Certificate Services**" progress bar appears. When Certificate Services has been started, a green "checkmark" will appear next to the CA icon in the **Certification Authority** interface.
15. If no further CA Administrator tasks are required, exit the **Certification Authority** interface and log out of the CA Administrator role.

Using **Certutil.exe** to restore the CA database:

1. Log on as the CA Administrator and stop Certificate Services. Log off.
2. Log on as an authorized CA Backup Operator.
3. Open a command line interface. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

4. Type:

certutil –restoreDB <BackupDirectory>

or

certutil –f -restoreDB <BackupDirectory>

Value	Description
-restoreDB	Specifies a restore of the CA's database.
BackupDirectory	Specifies the path where the backup data is stored.
-f	Forces an overwrite of the existing database.

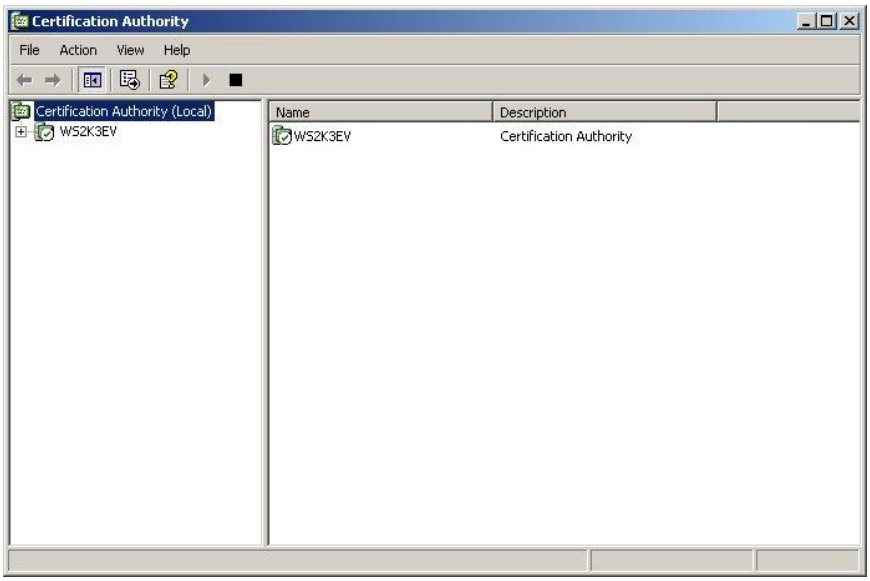
Configuring auditing of CA administrative actions

In order to log audit events related to CA administration activities, it is necessary to first enable the **Audit object access** security policy setting on the Windows Server 2003 host operating system. Procedures for enabling the host system's **Audit object access** security policy setting are provided in the Configuring Audit Policies subsection of this document. Once object access auditing is enabled on the host, explicit CA audit settings may be configured through the CA **Properties** interface.

Note: Within the TOE, the setting of selectable CA audit categories is optional, but highly recommended.

To configure auditing of CA administrative actions:

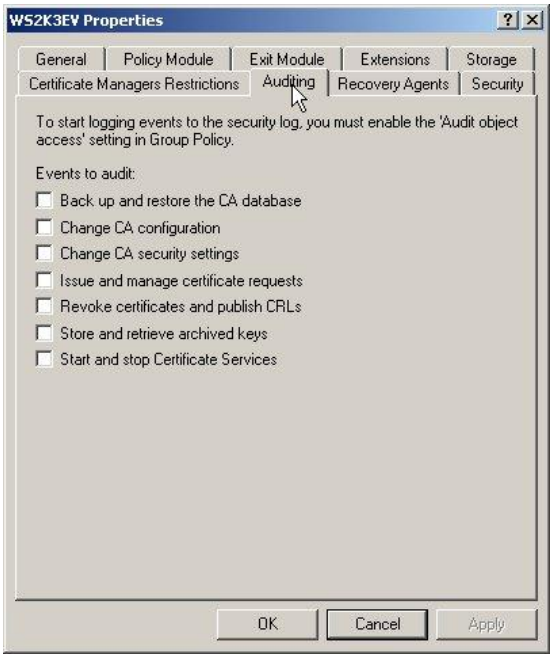
1. Log on to the server hosting the CA as an authorized CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.



3. In the console tree, right-click the name of the CA, point to **All Tasks**, and select **Properties**. The Certification Authority's **Properties** interface will appear.
4. Select the **Auditing** tab to display the auditable events.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. Select the event group to be audited by checking the box next to each event group listed under **Events to audit**.
6. If the **Start and stop Certificate Services** box is checked, a message will appear stating that when start and stop events are audited, the time that it will take to stop and start the Certificate Service will increase. Click **OK**.

7. After all audit selections are made, click **OK** in the **Properties** interface and close the **Certification Authority** snap-in.

The table below identifies the types of security events that will be logged to the operating system's security logs when specific CA related events are set for auditing. Table B-3 addresses only those events that are relevant within the TOE.

Table B-3 CA Audit Events

CA Event to Audit	Associated audit log Event ID / Description	Notes
Backup and restore the CA database	780. Certificate Services backup started. 781. Certificate Services backup completed. 782. Certificate Services restore started. 783. Certificate Services restore completed.	
Change CA configuration	788. Certificate Services imported a certificate into its database. 794. The Certificate Manager settings for Certificate Services changed for officer rights.	Addresses security-relevant data related to the configuration of Certificate Services, such as all changes to the trusted

Copyright © 2008 Microsoft Corporation.

All rights reserved.

CA Event to Audit	Associated audit log Event ID / Description	Notes
	795. A configuration entry changed in Certificate Services. 796. A property of Certificate Services changed. 800. One or more rows have been deleted from the certificate database. 802. Certificate Services template Records the information of a specific template when it is retrieved by the Certificate Server. 803. Certificate Services template updated Records the certificate information of a specific updated template when the updated template is retrieved by the Certificate Server. 804. Certificate Services template security updated Records the certificate information and the security descriptor of a specific updated template when the updated template is retrieved by the Certificate Server.	public keys, including additions and deletions and changes to the certificate Profile.
Change CA security settings	786. The security permissions for Certificate Services changed. 789. The audit filter for Certificate Services changed. 801. Role separation enabled.	Addresses security relevant data that is entered into the CA system including startup and shutdown of the audit function and any changes to the audit parameters, e.g., audit frequency, type of event audited. Any attempt to delete the audit log is addressed by audit events built into the Windows Server 2003 operating system. These audit events are addressed in the *Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0.*
Issue and manage certificate requests	772. The Certificate Manager denied a pending certificate request. 773. Certificate Services received a resubmitted certificate request. 777. A certificate request extension changed. 778. One or more certificate request attributes changed. 790. Certificate Services received a certificate request. 791. Certificate Services approved a certificate request and issued a certificate. 792. Certificate Services denied a certificate request. 793. Certificate Services set the status of a certificate request to pending.	Addresses all successful and unsuccessful requests for confidential and security relevant certificate information. Identifies certificate requests.

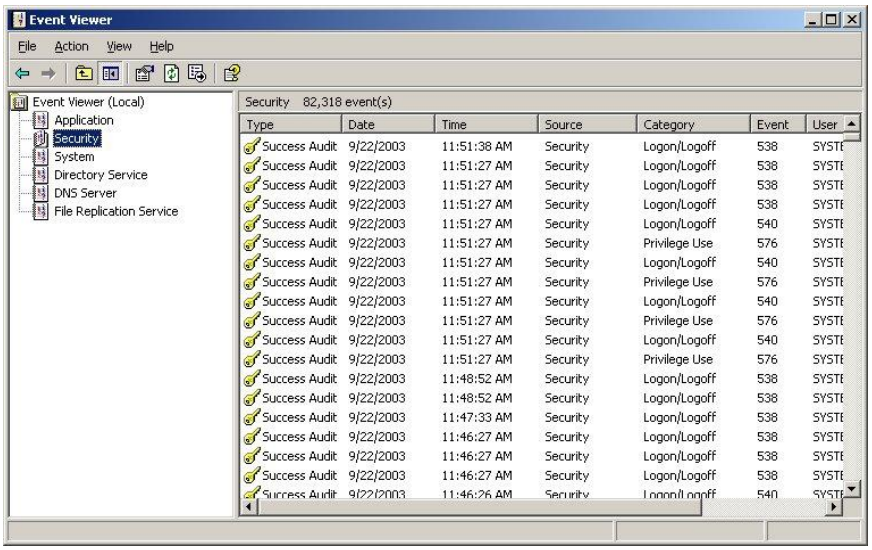
Copyright © 2008 Microsoft Corporation.

All rights reserved.

CA Event to Audit	Associated audit log Event ID / Description	Notes
	799. Certificate Services published the CA certificate to Active Directory.	
Revoke certificates and publish CRLs	774. Certificate Services revoked a certificate. 775. Certificate Services received a request to publish the CRL. 776. Certificate Services published the CRL.	Addresses all requests to change the status of a certificate and to change the certificate revocation list profile.
Start and stop Certificate Services	779. Certificate Services received a request to shut down. 784. Certificate Services started. 785. Certificate Services stopped.	

Viewing CA administrative audit events in the system security log

1. To view the system security log through **Event Viewer**, log on as an authorized CA Auditor. Click **Start**, point to **Programs**, point to **Administrative Tools**, and select **Event Viewer**.
2. In the **Event Viewer**, select the **Security** node. Security events will be displayed in the details pane.



3. To search the log for CA related security events, sort by event and look for any of the event IDs defined in Table B-3.
4. The event fields are described below in Table B-4.

Table B-4 Audit Event Fields

Event field	Description
Type	The event logs record five types of events: **Error** - A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event will be logged. **Warning** - An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event will be logged. **Information** - An event that describes the successful operation of an application, driver,

Copyright © 2008 Microsoft Corporation.

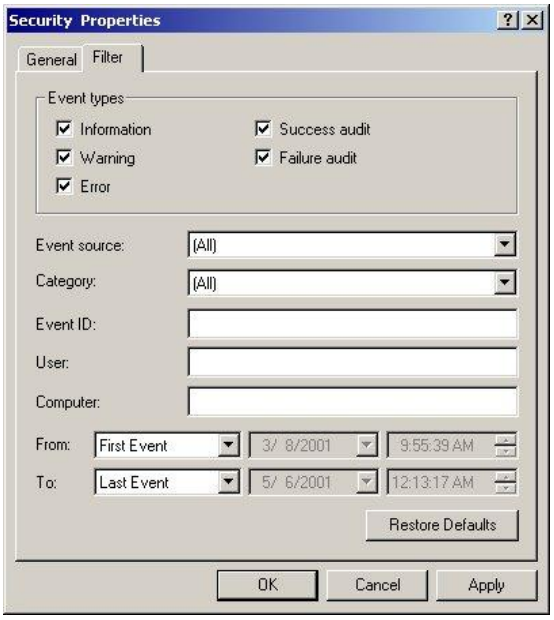
All rights reserved.

Event field	Description
	or service. For example, when a network driver loads successfully, an Information event will be logged. **Success Audit** - An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event. **Failure Audit** - An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.
Date	The date the event took place.
Time	The time the event took place.
Source	The process that raised the event.
Category	The specific class the event is categorized under.
Event	A unique numerical identifier for the event.
User	The user that generated the event.
Computer	The computer on which the event was generated.

5. **Event Properties** provide more information about events than the Events view. This additional information includes the event's source, a description of the event, and details about what is affected by the event. To view additional details for an event, select the event, right-click and select **Properties**. An **Event Properties** interface will appear.
6. The **Description** field of the **Event Properties** interface provides a longer explanation for the event, including what resources are affected and other technical information.
7. The **Properties** interface for the **Security** event log provides the ability to set filters on the event log to perform searches and sorting of audit data. To open the **Security Properties** interface, right-click on the Security node and select **Properties**.
8. To filter an existing event log in order to view or save specific security events, select the **Filter** tab and configure the filter.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



9. To configure the filter, select the **Event types** that will be included by checking or clearing a selection box next to **Information**, **Warning**, **Error**, **Success Audit**, and/or **Failure audit**, then input any additional desired filtering requirements by **Event source**, **Category**, **Event ID**, **User**, or **Computer**.
10. By default the entire event log will be filtered for viewing by the parameters selected above. If desired, select a date and time range for the logs that will be filtered for viewing. This is accomplished by first clicking on the **From:** drop down menu and changing the selection to **Events On**. The date and time dialog boxes will become active. Change the date by selecting the drop down menu and choosing a date from the calendar that is presented. Change the time by scrolling the up and down arrows in the time dialog box. Follow the same procedures clicking on the **To:** drop down menu and changing the selection to **Events On**. Set the date and time for the last as described above.
11. Once all the desired filtering options have been selected, click **OK**. The **Event Viewer** will filter the log and display the information as defined by the filter.

Note: For additional details on managing event logs, see the Audit Management subsection of this document.

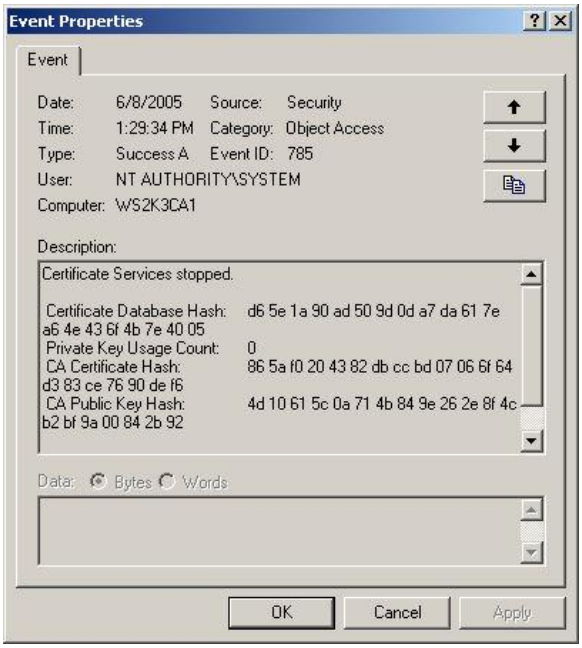
Using CA audit to verify the integrity of the CA after stopping and starting Certificate Services

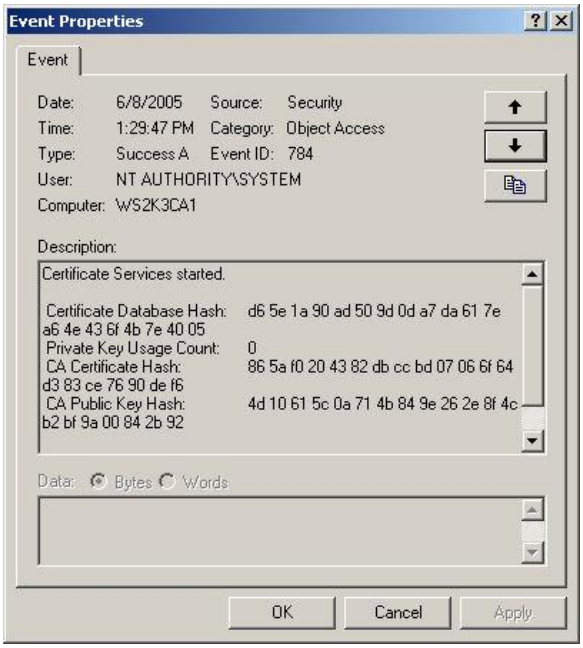
Enabling the **Start and stop Certificate Services** audit event category allows a CA Auditor to verify the integrity of the certificate database. When the CA is started, and when it is stopped, hashes of the certificate database, the CA public key and the CA certificate are created. These three hash values and a Certificate Service private key usage count are included with the start and stop event when it is recorded in the IT Environment security event log. The hash values from the most recent Certificate Service start and stop events can be compared to ensure the database was not altered when the service was not running.

The CA Auditor can verify the integrity of the CA by analyzing the cryptographic hash values recorded in the **Security** events log in order to compare the hash values in the last Event ID 785 (Certificate Services stopped) event record with the most recent Event ID 784 (Certificate Services started) event record. Within the TOE, the Private Key Usage Count entry may appear as 0 since the CA's private key is secured by the Hardware Security Module (HSM).

Copyright © 2008 Microsoft Corporation.

All rights reserved.





Renewing CA Certificates

A certification authority may need to be renewed for either of the following reasons:

- Change in the policy of certificates issued by the CA
- Expiration of the CA's issuing certificate

Certification authority validity periods

Before discussing the renewal of a CA certificate, it is helpful to understand how the end of the validity period of a CA affects the validity period of the certificates it issues. Certificate Services enforces a rule that a CA never issues a certificate to be valid beyond the expiration date of its own certificate. Therefore, when a CA's certificate reaches the end of its validity period, all certificates it has issued will also expire. This way, if the CA is purposely not renewed and the CA reaches the end of its lifetime, a PKI administrator can be assured that all the certificates that the now-expired CA has issued can no longer be used as valid security credentials. In other words, there will be no "orphaned" certificates that are still within their validity period but which have been issued by a CA that is no longer valid.

To illustrate how a decreasing validity period works, consider the following scenario: An organization installs a root CA with a certificate validity period of five years. The organization then uses this root CA to issue certificates with a validity period of two years to subordinate CAs. For the first three years every certificate issued to a subordinate CA by the root CA will continue to have a validity period of two years. After three years, when there is less than two years left in the validity period of the root CA certificate, Certificate Services begins to reduce the validity period of the certificates issued by the root CA so that they do not exceed the end of the CA's certificate's expiration date. Therefore, after four years, the CA issues subordinate CA certificates that are valid for one year. After 4.5 years, issued subordinate CA certificates have a validity period of only six months.

Certificate Services allows the following maximum validity periods that are based on the type of certificate. These validity periods are configurable by the Domain Admin or Enterprise Admin when using version 2 certificate templates:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Table B-5 Certificate Validity Periods

Type of Certificate	Maximum Validity Period
Root CA	Specified during setup of Certificate Services
Subordinate CA, Internet Protocol Security, Enrollment Agent, Domain Controller	Up to 5 years, never more than the Root CA's validity period
All other certificates	1 year, never more than the Root CA's validity period

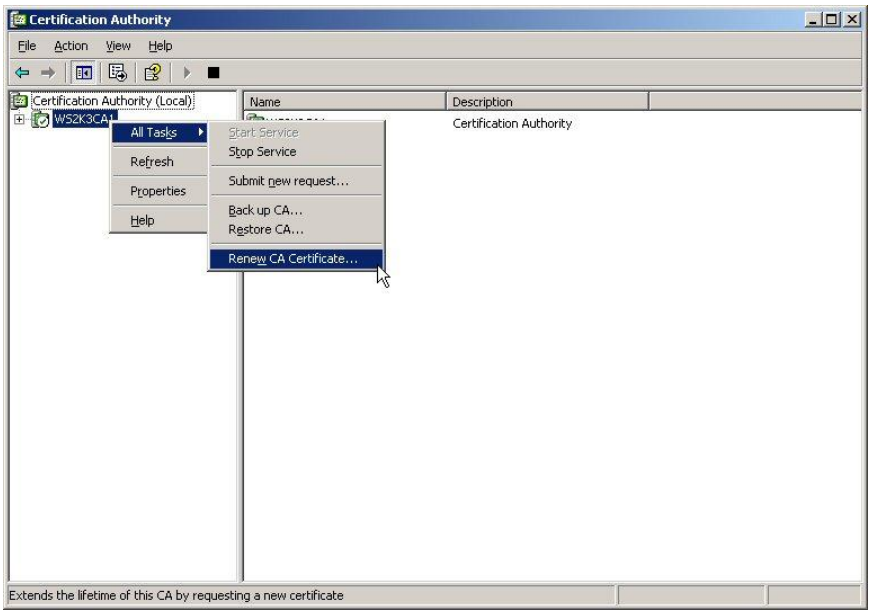
Since a CA that is approaching the end of its own validity period issues certificates valid for shorter and shorter periods of time, it is recommended to have a plan in place to renew the CA certificate well before it expires in order to avoid issuing certificates of a very short validity period.

One renewal consideration: When renewing a CA, there is the option of reusing its existing key pair or generating a new key pair. When a new key pair is generated for a CA that is being renewed, a new CRL distribution point is also created. This is to ensure that the key used to sign a certificate issued by the CA also matches the key used to sign the CRL.

Renewing a root CA's certificate

A root CA issues its own certificate, therefore all certificates are requested, generated, and issued locally. To renew a root CA certificate:

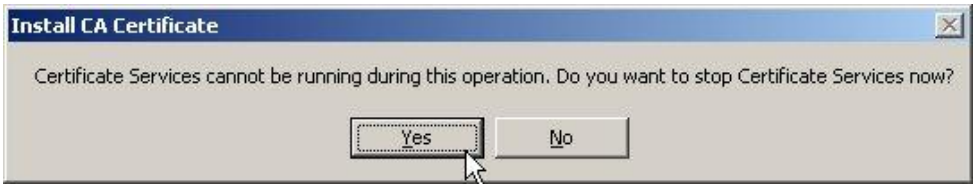
1. Log on to the CA host as an authorized IT Administrator.
2. Open the **Certification Authority** interface for the Root CA. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right click the CA, select **All Tasks**, and then select **Renew CA Certificate**.



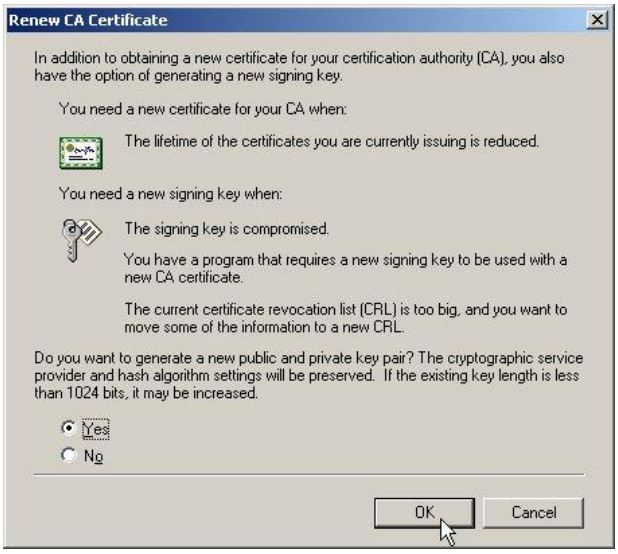
4. A message will appear stating that Certificate Services cannot be running during the renewal operations. Click **Yes** to stop Certificate Services.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. A **Renew CA Certificate** interface will appear. It explains that in addition to generating a new CA certificate there is also an option of generating a new signing key. Read the information provided in the window to determine if a new signing key is required. If so, then select the **Yes** radio button and click **OK** to generate a new public and private key pair. If a new signing key is not required select the **No** radio button on the **Renew CA Certificate** interface and click **OK** to continue.



Note: If **Yes** is selected on the **Renew CA Certificate** interface, an additional message will appear asking if it is OK to overwrite the private key with a new one. If the **No** button is selected, the certificate renewal operation will be aborted. If the **Yes** button is selected, the renewal request operation will continue.

6. A new CA certificate will be generated and Certificate Services will be restarted. Close the **Certification Authority** interface if no further action is required.

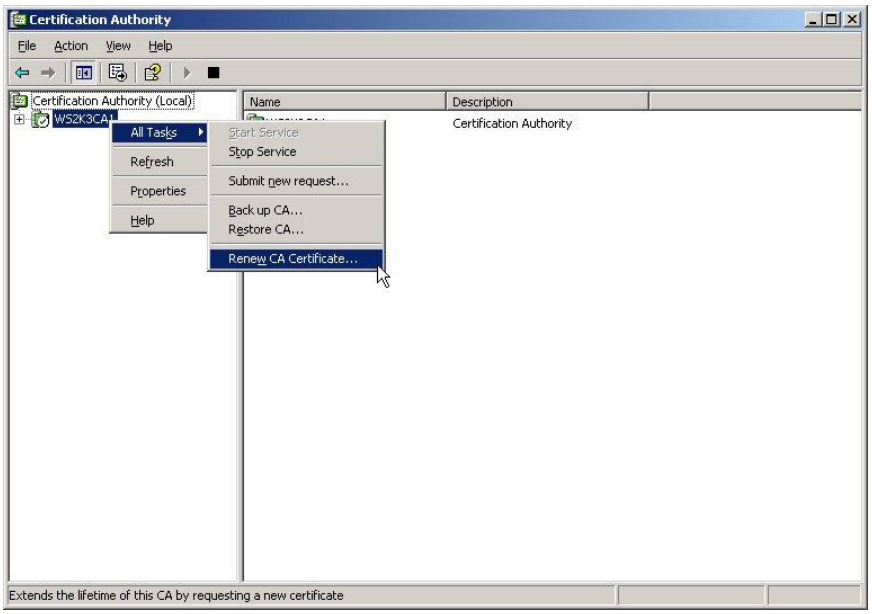
Renewing a subordinate CA's certificate

To renew a subordinate CA certificate:

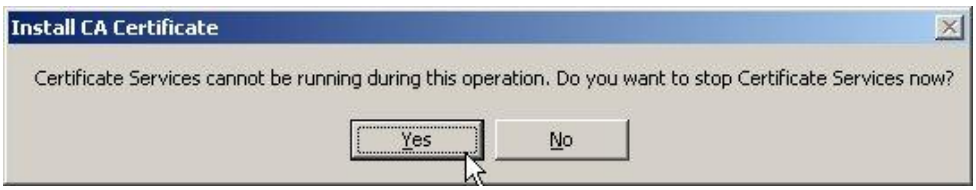
1. Log on to the CA host as an authorized IT Administrator.
2. Open the **Certification Authority** interface for the Root CA. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right click the CA, select **All Tasks**, and then select **Renew CA Certificate**.

Copyright © 2008 Microsoft Corporation.

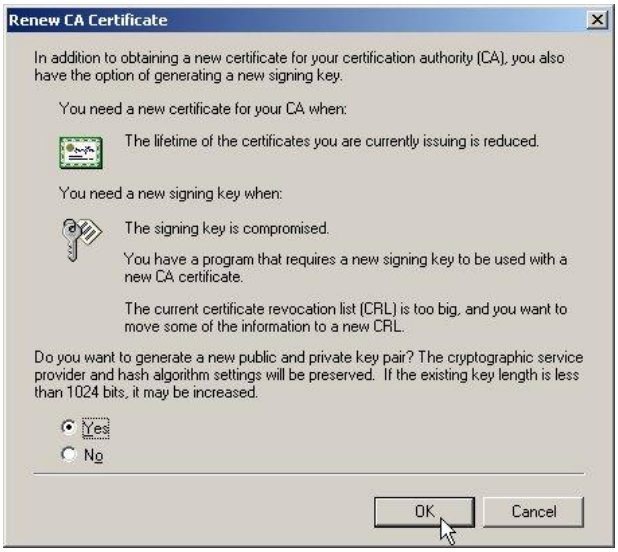
All rights reserved.



4. A message will appear stating that Certificate Services cannot be running during the renewal operations. Click **Yes** to stop Certificate Services.



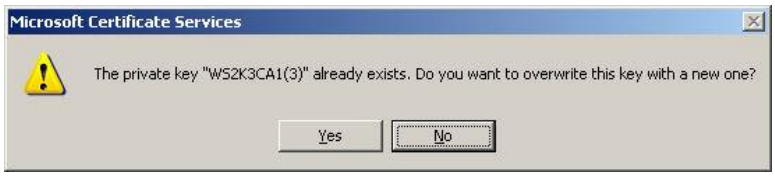
5. A **Renew CA Certificate** interface will appear. It explains that in addition to generating a new CA certificate there is also an option of generating a new signing key. Read the information provided in the window to determine if a new signing key is required. If so, then select the **Yes** radio button and click **OK** to generate a new public and private key pair. If a new signing key is not required select the **No** radio button on the **Renew CA Certificate** interface and click **OK** to continue.



Copyright © 2008 Microsoft Corporation.

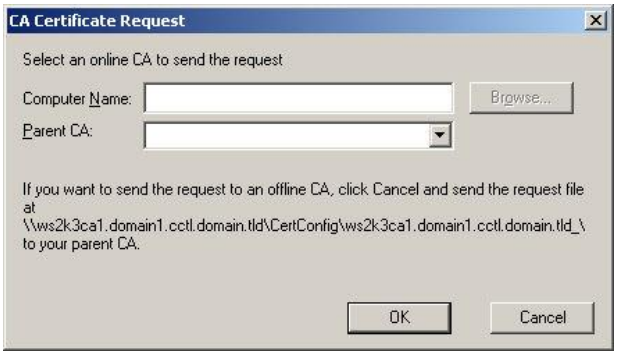
All rights reserved.

Note: If **Yes** is selected on the **Renew CA Certificate** interface, an additional message may appear asking if it is OK to overwrite the private key with a new one.



If the **No** button is selected, the certificate renewal operation will be aborted. If the **Yes** button is selected, the renewal request operation will continue.

6. A **CA Certificate Request** interface will appear.



- If the parent CA is available online, type the name of the computer on which the parent CA is installed in the **Computer Name** entry field, then use the pull-down menu for the **Parent CA** entry field to select the parent CA.
- If the parent CA is not online, click **Cancel** and manually transfer the certificate request to the parent CA. The certificate request file can be found in the CertConfig share folder.

7. If the parent CA is accessible from the network, the subordinate will receive the certificate once it is issued from the parent CA.
8. If the parent CA is not accessible from the network, follow the procedures below to import the CA certificate once it is received from the parent. Procedures for getting a CA certificate from an offline root are in the "Obtaining a CA certificate from an offline parent CA" subsection.

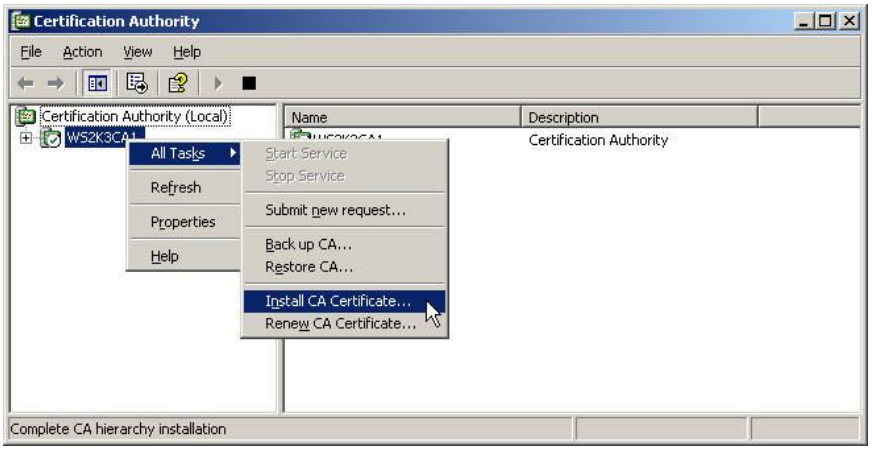
Note: If the subordinate CA certificate does not include the full certification path, install a valid CA chain when it starts. Install the parent CA's certificate in the Intermediate Certification Authorities certificate store of the computer (if the parent CA is not a root CA), as well as the certificates of any other intermediate CA in the chain, and install the certificate of the root CA in the chain into the Trusted Root Certification Authorities store. These certificates should be installed in the certificate store before installing the CA certificate on the subordinate CA. If these certificates are still valid, they do not need to be reinstalled to support the subordinate CA's certificate renewal.

Install the subordinate CA's certificate:

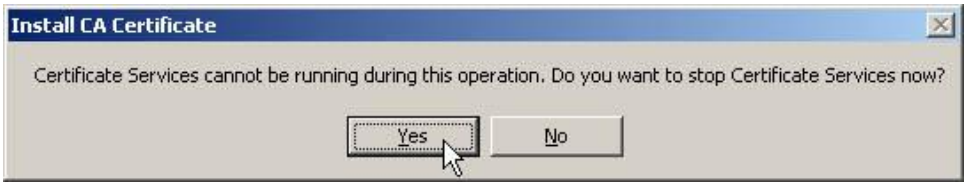
1. Log on to the CA host as an authorized IT Administrator.
2. At the Subordinate CA, open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Right-click the node representing the CA, point to **All Tasks** and select **Install CA Certificate**.

Copyright © 2008 Microsoft Corporation.

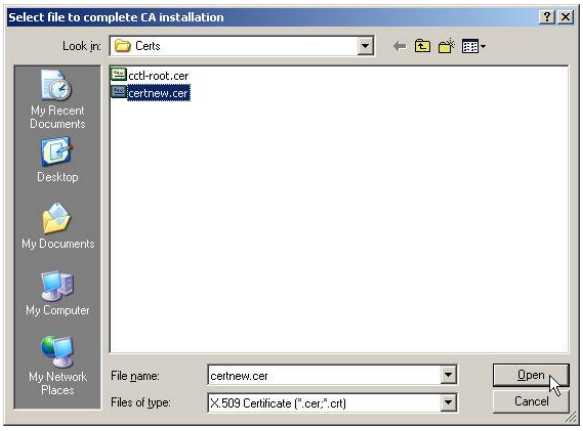
All rights reserved.



4. If Certificate Services was not previously stopped, a message will appear stating that the service cannot be running during the certificate installation operation. Click **OK**. Certificate Services will be stopped.



5. Locate the certificate file received from the parent certification authority, select the file, and then click **Open**.



6. The certificate will be installed and Certificate Services will be restarted.
7. If Certificate Services does not automatically start, right-click the node representing the CA, point to **All Tasks** and select **Start Service**.

Obtaining a Subordinate CA certificate from an offline parent CA

Offline root CAs are outside the TOE but may be used to issue subordinate CA certificates to a CA within the TOE. To obtain a certificate from an offline root CA, follow the procedures specified by the vendor of the offline root CA product. If the offline root CA is a Microsoft Server 2003 Certificate Server, the subordinate CA certificate may be obtained by following procedures on the Certificate Services Web pages, if IIS is installed on the offline root CA, or by using the certutil.exe command line utility. For

Copyright © 2008 Microsoft Corporation.

All rights reserved.

example, to submit a CA certificate request and retrieve the issued certificate on a Windows Server 2003 Certificate Server offline root CA using the certutil.exe command line utility:

1. Log on to the offline CA host as an authorized CA Certificate Manager and insert the media containing the certificate request file.
2. Open a command line interface. Click **Start**, point to **All Programs**, point to **Accessories**, and select **Command Prompt**.

   Note: Change directories to the location of the certificate request file, if the media is writable. Otherwise copy the request file to a local folder and change directories to that folder location.

3. To submit a certificate request, use **certreq.exe** in the following command string format:

   certreq –Submit <request file name>

4. For example, if the name of the request file (generated previously by using the Certification Authority interface) is ***WS2K3CA1.WS2K3Lab1.com_WS2K3CA1.req***, enter the following command and hit the Enter key:

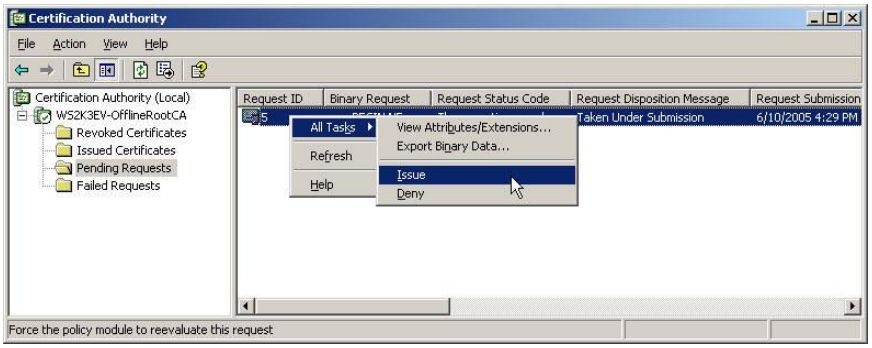
   certreq –Submit WS2K3CA1.WS2K3Lab1.com_WS2K3CA1.req

5. The Select Certification Authority interface will appear. Select the CA and click the **OK** button.

6. A **RequestId** number will be shown in the command line interface and a message may indicate that the request is taken under submission. Take note of the **RequestId** number.

   Note: By default, certificates are not automatically issued by Stand-alone CAs (used for offline CAs).

7. Open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
8. Expand the CA node, and then select the Pending Requests folder. Right-click on the recently submitted certificate request, point to **All Tasks** and select **Issue**.



9. Return to the command line interface to retrieve the issued certificate. To retrieve an issued certificate, use **certreq.exe** in the following command string format:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

certreq –Retrieve <RequestId number> <cert output file name>

10. For example, if the name of the **RequestId** number is **5**, and the desired output file is ***WS2K3CA1.cer***, enter the following command and hit the Enter key:

certreq –Retrieve 5 WS2K3CA1.cer

11. The Select Certification Authority interface will appear. Select the CA and click the OK button.

12. A message will appear indicating that the certificate was issued. Take the certificate file to the subordinate CA and follow the procedures in the "Renewing a subordinate CAs certificate" subsection to install it.

Note: For additional details and options for using certreq.exe, enter **certreq -?** at the command line.

Viewing a CA Certificate

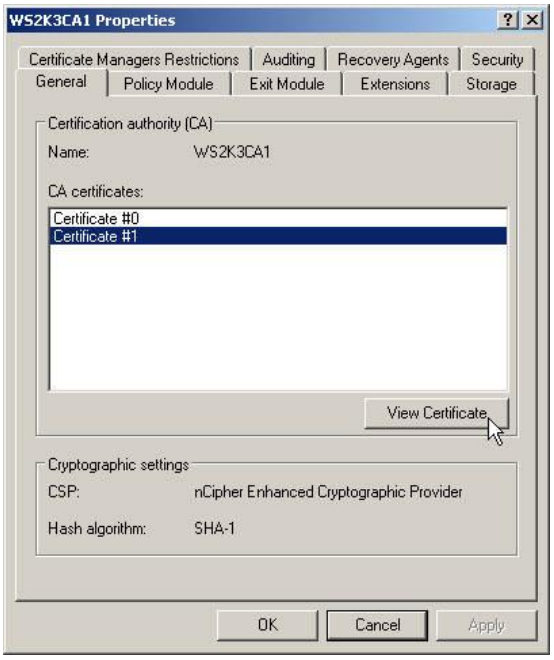
To view the CA's Certificate:

1. Log on to the computer using any CA management role.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then select **Certification Authority**.
3. Right-click the CA node and select **Properties**.
4. Select the certificate to view and click the **View Certificate** button on the **General** tab view of the CA **Properties** interface,

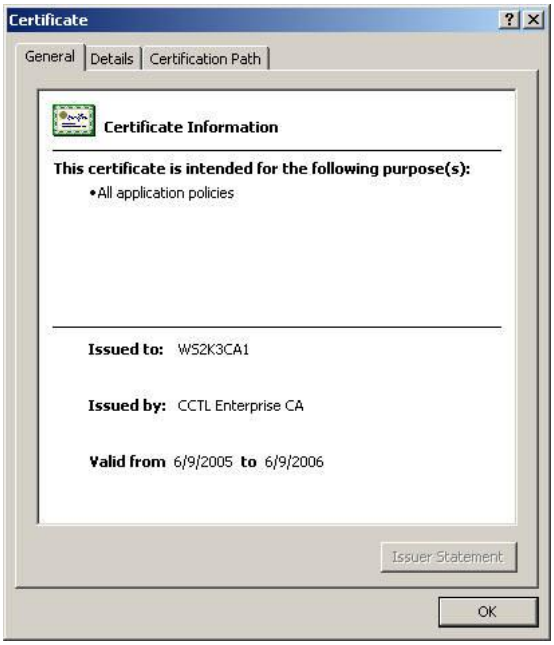
Note: If the CA's certificate has been renewed, there may be more than one certificate displayed in the CA certificates display. The latest certificate will be the lowest on the list and has the highest number (#) value.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



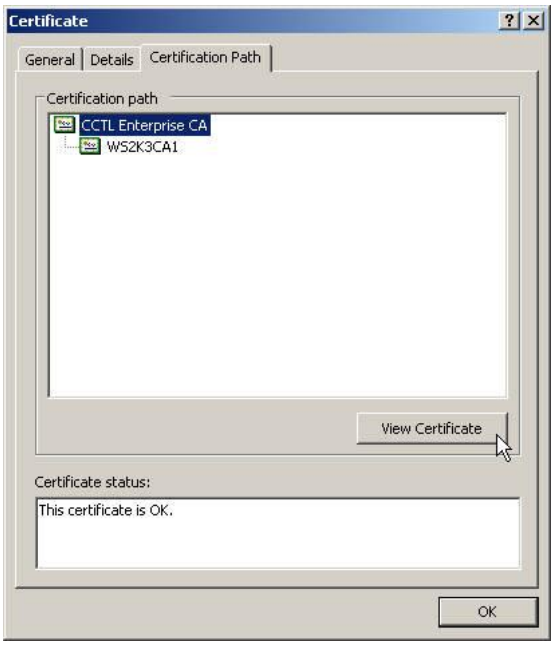
5. The CA's certificate will be displayed. To view certificate details click the **Details** tab.



6. To view the parent CA's certificate, click the **Certification Path** tab. The parent CA's certificate may be viewed by selecting it and clicking the **View Certificate** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Managing Certificate Revocation

A CRL is a digitally signed document maintained and published by a certification authority that lists certificates that have been revoked. A delta CRL is a digitally signed document of the changes that have occurred since the issuance of the prior base CRL. The Certificate Server generates CRLs and delta CRLs using templates implemented directly in code. The value of the Issuer field and Issuer Alternative Name extension field is determined when the CA is initially configured as defined in Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide.

Revoking a certificate

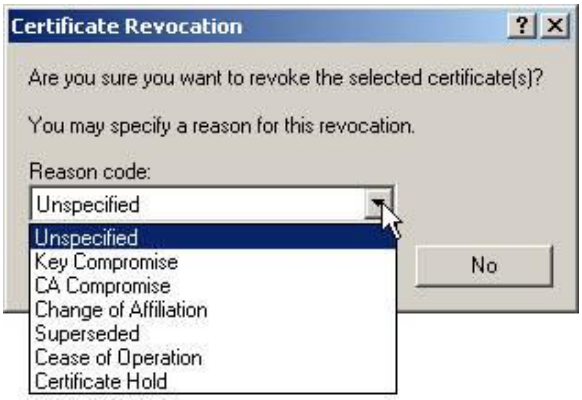
To help maintain the integrity of an organization's PKI, a certificate must be revoked if a user leaves the organization, if the certificate subject's private key has been compromised, or if some other security-related event dictates that it is no longer desirable to have a certificate considered "valid." When a certificate is revoked, it is added to the CA's CRL. This may take the form of a new CRL or a delta CRL, which is a small CRL that lists the certificates that have been revoked since the last full CRL.

To revoke an issued certificate:

1. Log on to the computer as a Certificate Manager.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then select **Certification Authority**.
3. Expand the CA node. Select the **Issued Certificates** folder then right-click on the certificate that is to be revoked and select **Revoke Certificate**.
4. On the **Certificate Revocation** interface, select a **Reason code** from the drop down menu and click **Yes**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. The certificate will be revoked and will appear in the **Revoked Certificates** folder of the **Certification Authority**. The revoked certificate will appear on the CRL the next time it is published.

Unrevoking a certificate

Once revoked, certificates can only be unrevoked if they were revoked with the **Certificate Hold** reason code. Attempts to unrevoke certificates with any other reason code will result in the following message

To unrevoke a certificate that was revoked with the **Certificate Hold** reason code:

1. Log on to the computer as a Certificate Manager.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then select **Certification Authority**.
3. Expand the CA node. Select the **Revoked Certificates** folder then right-click on the certificate that is to be unrevoked and select **Unrevoke Certificate**.
4. The certificate will appear in the **Issued Certificates** folder.

Publication of CRLs and Delta CRLs

Windows Server 2003 Certificate Server automatically publishes an updated CRL after an interval of time specified by the CA Administrator. This interval of time is known as the CRL "publication interval." After the initial setup of a CA, the CRL publication interval is set to one week (based upon the local computer's time, starting from the date when the CA is first installed).

A CA Administrator should understand that there is a difference between a CRL publication interval and the validity period of a CRL. The validity period of a CRL is the period of time that the CRL is considered authoritative by a verifier of a certificate. As long as the verifier of a certificate has a valid CRL in its local cache, it will not attempt to retrieve another CRL from the CA which publishes it.

The publication interval of a CRL is established by the CA administrator. However, the validity period of the CRL is extended from the publication interval to allow for Active Directory replication. By default, Certificate Services extends the publication interval by 10% (up to a maximum of 12 hrs) to establish the validity period. So, for example, if a CA is publishing a CRL every 24 hours, the validity period is set to 26.4 hours.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Additionally, there is a clock skew of an additional 10 minutes added to the validity period on either side of the publish period, so a CRL will be valid 10 minutes before the beginning of its publish period to account for variances in computer clock settings. There are registry entries which allow an administrator to control the variance between the publication interval and validity period to allow for slower directory replication.

Note: Within the TOE, the **ClockSkewMinutes** registry value is set at **1** minute. For details on setting the **ClockSkewMinutes** registry value see the "Adjusting the clock skew Registry settings" subsection below.

When determining the schedule for the CRL publication interval, there is a trade-off between performance and security. The more often CRLs are published, the more current clients can be with the list of revoked CRLs and the less likely they are to accept recently revoked certificates. However, frequent publishing can negatively impact network and client performance. To help mitigate this trade off, delta CRLs can be used if the environment supports them.

Since clients will normally have the CRL cached locally, the use of delta CRLs can potentially improve performance. To use delta CRLs, the client application must be aware of and explicitly use delta CRLs for revocation checking. If the client does not use delta CRLs, it will retrieve the CRL from the CA every time it refreshes its cache, regardless of whether a delta CRL exists or not. For this reason, administrators should verify that the intended applications use delta CRLs and configure the CA accordingly. If the clients do not support the use of delta CRLs, administrators should either not configure the CA to publish delta CRLs or configure it so CRLs and delta CRLs are published at the same interval. This would still allow future applications that support delta CRLs to use them, while providing current CRLs to all applications. Note that all applications that use CryptoAPI in Windows XP and the Windows Server 2003 family use delta CRLs.

Adjusting the clock skew registry settings

The **ClockSkewMinutes** registry value controls the time variance allowed for certificate issuance, certificates, and CRLs. If the times on the clocks on two computers are further apart than this registry setting, a newly enrolled certificate will not be immediately valid and the client will have to wait several minutes before being able to use the new certificate. The default setting is 10 minutes, however, within the TOE this setting is changed to 1 minute.

To verify the **ClockSkewMinutes** registry setting:

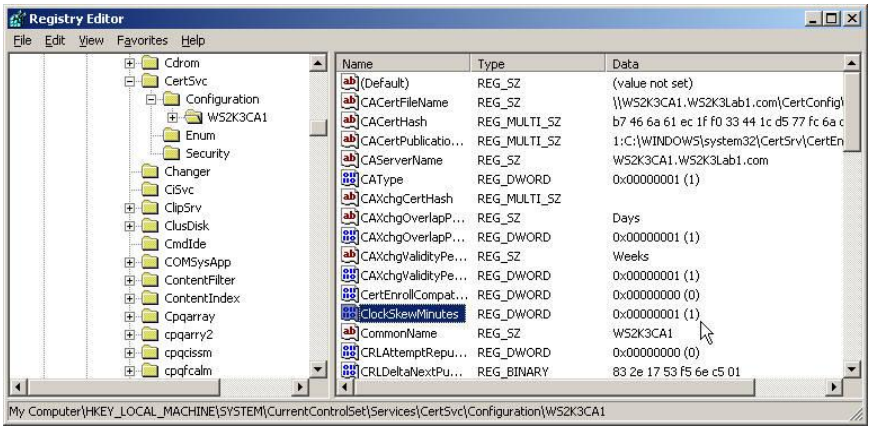
1. Log on to the computer as an authorized Administrator.
2. Click **Start** and select **Run**. Type **regedit** and click **OK**.
3. Navigate the **Registry Editor** to find and select the following key path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CAName>

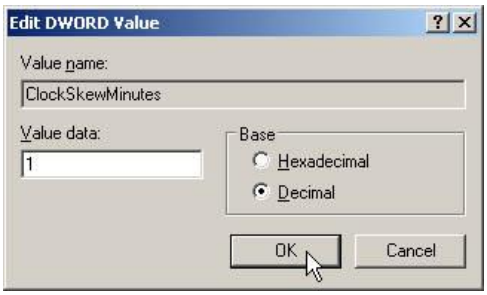
4. Verity that the **ClockSkewMinutes** value is set to **1** minute.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



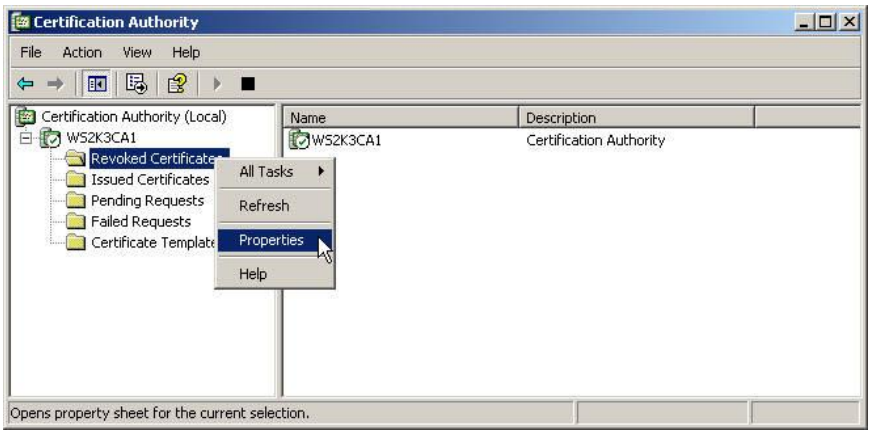
5. If the value needs to be modified, double-click on the **ClockSkewMinutes** registry value. On the **Edit DWORD Value** interface, select the **Decimal** radio button, enter a **1** in the Value data field and click **OK**.



Scheduling the publication intervals of CRLs and Delta CRLs

Schedule when the CRL and Delta CRLs are published using the following procedure:

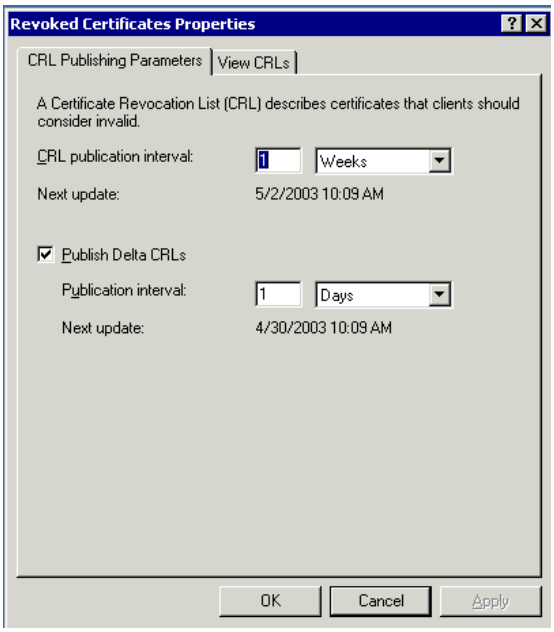
1. Log on to the computer as a CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then select **Certification Authority**.
3. Expand the CA node. Right click the **Revoked Certificates** folder and select **Properties**.



4. Select **the CRL Publishing Parameters** tab.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. In **CRL publication interval**, type the increment and select the unit of time to use for the automatic publishing of the CRL.
6. To change the **Next Update** field in a Delta CRL, check the **Publish Delta CRLs** checkbox.
7. In **Publication interval**, type the increment and select the unit of time to use for the automatic publishing of the delta CRL.

Defining Delta CRL publishing parameters has the effect of issuing Delta CRLs that include the Delta-CRL Indicator Extension Field. This field indicates that this is a Delta CRL and identifies the CRL number of the base CRL to which the changes in this Delta CRL should be applied.

Notes:

- If the computer is a domain member and has permission to write to the Active Directory service, then the CRL and Delta CRLs are also published to Active Directory.
- The publishing period for a CRL is not the same as the validity period for a CRL. By default, the validity period of a CRL exceeds the publishing period of a CRL by 10% (up to a 12-hour maximum) to allow for directory replication.

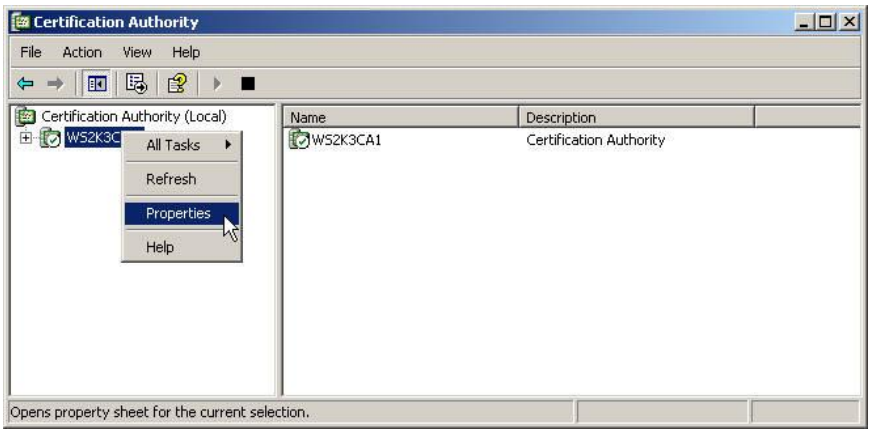
Modifying the Certificate Revocation List Distribution Points Extension Field

CRL Distribution Points (CDPs) are used in certificates to identify where the CRL associated with a certificate is located. CDPs in CRLs help to prevent the possible substitution of one CRL with another. CA Administrators have the option to include CDPs in CRLs. This is accomplished using the following procedure:

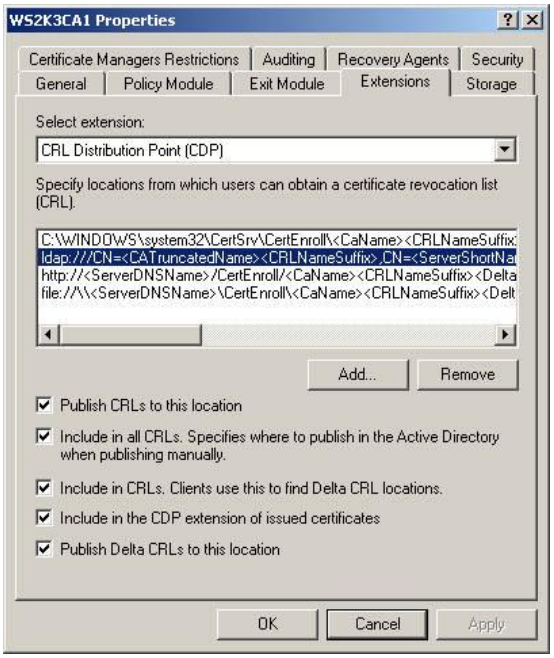
1. Log on to the computer as a CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then select **Certification Authority**.
3. In the console tree, right-click the CA node and select **Properties**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



4. On the CA **Properties** interface, select the **Extensions** tab.



5. Confirm that Select extension is set to CRL Distribution Point (CDP).
6. To make changes or additions to the list of CDPs, do one or more of the actions shown in the Table B-6 below.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Table B-6 Procedures for Modifying CDPs

To	Do this
Add a new CDP.	Click **Add**, type the name of the new CDP, and click **OK**.
Remove a CDP from the list.	Select the CDP from the list in the **Specify locations from which users can obtain a certificate revocation list (CRL)** box, and then click **Remove** and click **OK**.
To use a Uniform Resource Locator (URL) address as a CDP.	Select the CDP representing the URL, select the **Include in the CDP extension of issued certificates** check box, and then click **OK**.
To stop using a URL as a CDP.	Select the CDP representing the URL, clear the **Include in the CDP extension of issued certificates** check box, and then click **OK**.
To use a URL as a delta CDP.	Select the CDP representing the URL, select the **Publish Delta CRLs to this location** check box, and then click **OK**.
To stop using a URL as a delta CDP.	Select the CDP representing the URL, clear the **Publish Delta CRLs to this location** check box, and then click **OK**.
To publish a location in CRLs to point clients to a delta CRL.	**Select the CDP, select the Include in CRLs. Clients use this to find Delta CRL locations** check box, and then click **OK**.
To not publish a location in CRLs to point clients to a Delta CRL.	Select the CDP, clear the **Include in CRLs. Clients use this to find Delta CRL locations** check box, and then click **OK**.

7. Click **Yes** to stop and restart the Certificate Services service.

Certificate revocation list URLs can be HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Lightweight Directory Access Protocol (LDAP), or file addresses. Use the variables shown in Table B-7 when specifying the address of the CRL.

Table B-7 CRL Address Variables

Variable	Description
CAName	The name of the certification authority.
CAObjectClass	The object class identifier for a certification authority, used when publishing to an LDAP URL.
CATruncatedName	The "sanitized" name of the certification authority, truncated to 32 characters with a hash on the end.
CDPObjectClass	The object class identifier for CRL distribution points, used when publishing to an LDAP URL.
CertificateName	The renewal extension of the certification authority.
ConfigurationContainer	The location of the Configuration container in Active Directory.
CRLNameSuffix	Inserts a name suffix at the end of the file name when publishing a CRL to a file or URL location.
DeltaCRLAllowed	When a delta CRL is published, this replaces the CRLNameSuffix with a separate suffix to distinguish the delta CRL.
ServerDNSName	The Domain Naming System (DNS) name of the certification authority server.
ServerShortName	The NetBIOS name of the certification authority server.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

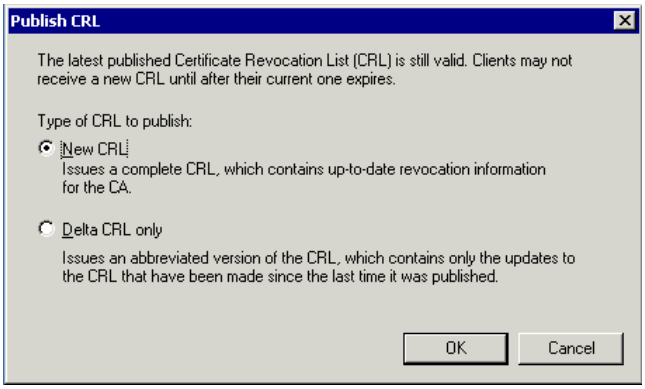
Publishing a CRL before the next scheduled publish period

A CRL can be published at any time, such as when a valuable certificate becomes compromised. Choosing to publish a CRL outside the established schedule resets the scheduled publication period to begin at that time. In other words, if a CRL is manually published in the middle of a scheduled publish period, the CRL publish period is restarted.

It is important to realize that clients that have a cached copy of the previously published CRL will continue using it until its validity period has expired, even though a new CRL has been published. Manually publishing a CRL does not affect cached copies of CRLs that are still valid; it only makes a new CRL available for systems that do not have a cached copy of a valid CRL.

To manually publish the CRL:

1. Log on to the computer as a CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node. Right-click the **Revoked Certificates** folder, point to **All Tasks** and select **Publish**. A **Publish CRL** selection interface will appear.



4. Select the **Type of CRL to publish**. Select **New CRL** to publish a complete CRL or select **Delta CRL** only to publish an abbreviated version of the CRL which only contains the updates since the last published CRL.
5. Click **OK** to publish the CRL.

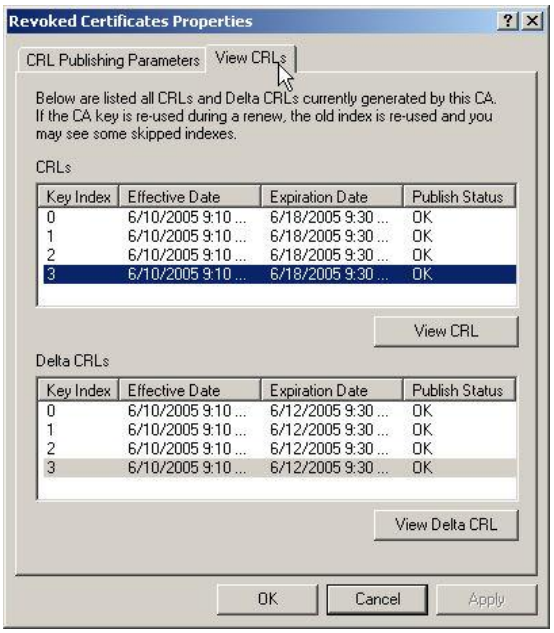
Viewing CRLs

View the published CRL to verify that it is correct.

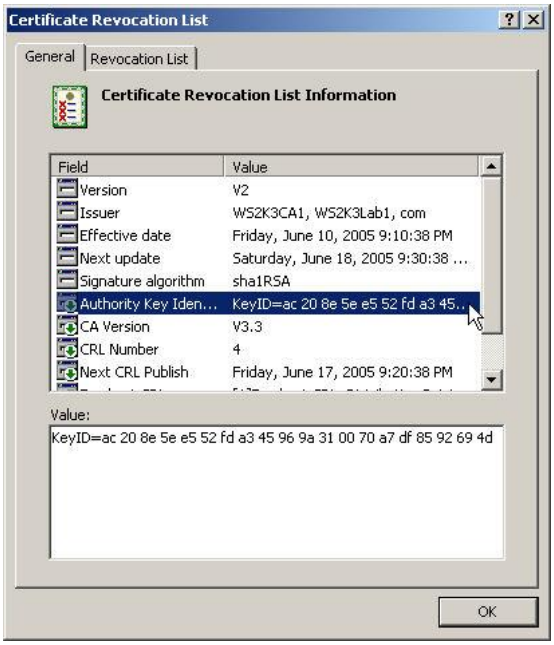
1. Log on to the computer using any of the authorized CA roles.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. In the console tree, right-click the **Revoked Certificates** node and select **Properties**.
4. On the **Revoked Certificates Properties** interface, select the **View CRLs** tab. Select a CRL from the CRLs list and click the **View CRL** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. The **Certificate Revocation List** interface displays, providing overall identification information for the CRL. To view the CRL contents, click the **Revocation List** tab.



6. To view details on a particular revoked certificate in the **Revocation List**, select it. The details are displayed in the **Revocation Entry** box. The **Value** box is provided in case the field values are too large for the Field/Value pair. Selecting one of the **Field** entries displays the full contents of the selected field.

Revoking Large Numbers of Certificates

When a large number of certificates are revoked, such as during an employee layoff, the Delta CRL size may increase significantly due to the large number of entries, and almost all clients will refer to the older

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Base CRL. This situation will happen even if a new base CRL is published right after the revocation of the certificate until the new base is fully propagated.

To overcome the scenario where the Delta CRL is very large, perform the following steps on the CA.

1. Modify the registry values under the following registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<CAName>

   - Set the **CRLOverLapPeriod** value to **Minutes**. The default is hours.
   - Set the **ClockSkewMinutes** value to **1**. The default is 10, but within the TOE it is already set at 1.
2. Restart the CA.
3. Publish a new Base CRL. The Base CRL will have a CRLPropagationComplete time that will be just two minutes and any subsequent Delta CRLs will refer to this base CRL.
4. Once this has been completed, restore the CRLOverLapPeriod to the default values.

Managing Certificate Requests

In Windows Server 2003, a certificate request can be driven from at least three different sources. The sources built into the operating system are the Web browser (Internet Explorer), the **Certificate Request Wizard**, and auto-enrollment. All three methods call xenroll.dll (Microsoft Enrollment Control), which provides various methods to support certificate request generation and certificate installation[7].

A security principal can manually or automatically request a certificate from a Windows Server 2003 CA. This request is held until administrative approval is received from the Certificate Manager or the verification process is completed. Once the certificate has been approved or issued, the process will complete and install the certificate automatically.

Allowing enrollment and autoenrollment for certificates

For details and procedures to allow a specific security principal to enroll or autoenroll for certificates based on a certificate template, see the Allow subjects to request a certificate based on a template and Security subsections. Additional configuration settings affecting autoenrollment are discussed below.

Configuring autoenrollment

Autoenrollment is a useful feature of certification services in Windows XP and Windows Server 2003. Autoenrollment allows subjects to automatically enroll for certificates, retrieve issued certificates, and renew expiring certificates without requiring subject interaction. The subject does not need to be aware of any certificate operations, unless the CA Administrator configures the certificate template to interact with the subject.

[7] Web browser based method of requesting a certificate is not used within the TOE.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

To properly configure subject autoenrollment, the CA Administrator must plan the appropriate certificate template or templates to use. Several settings in the certificate template directly affect the behavior of subject autoenrollment.

- On the **Request Handling** tab of the selected certificate template, the selection of an autoenrollment user interaction setting will affect autoenrollment:
  - **Enroll subject without requiring any user input**. This setting will allow "silent" autoenrollment without requiring the user to take any action. This setting is preferred when clients require certificates but may not be aware that they are using them.
  - **Prompt the user during enrollment**. The user will receive a message and may need to take an action when enrollment is performed. This action may be necessary when the certificate is intended for a smart card, which would require the user to provide their personal identification (PIN).
  - **Prompt the user during enrollment and require user input when the private key is used**. This setting prompts the user both during enrollment and whenever the private key is used. This is the most interactive autoenrollment behavior, as it requires the user to confirm all use of the private key. It is also the setting that provides the highest level of user awareness regarding key usage.
- On the **Request Handling** tab of the selected certificate template, the number of Cryptographic Service Providers (CSPs) that are selected in the CSP Selection list box changes the behavior of autoenrollment for smart card templates. If more than one smart card CSP is selected, users may receive more than one dialog box when the autoenrolled certificate is retrieved and begins to install it on the smart card. It is recommended that only one CSP be selected from this list for each template.
- On the **Subject Name** tab of the selected certificate template, selecting the **Supply in the request** option disables autoenrollment based on this template. Enabling the option prompts the subject to interactively create the subject name in the request, which will not work with autoenrollment.
- On the **Issuance Requirements** tab of the selected certificate template, selecting **This number of authorized signatures** and making the value greater than **1** disables subject autoenrollment based on this template.
- On the **Issuance Requirements** tab of the selected certificate template, selecting **This number of authorized signatures** and setting the value to **1** requires the requestor to sign the request with a private key from a valid certificate in their certificate store. This certificate must contain the application and issuance policies that are specified in the **Application policy** and *Issuance policies* lists on the same tab. If an appropriate certificate exists in the requestor's certificate store, autoenrollment signs the request with this certificate's private key and obtains and installs the requested certificate automatically.
- On the **Issuance Requirements** tab of the selected certificate template, the **Valid existing certificate** option may affect subject autoenrollment. This option tells the CA that the subject does not need to meet issuance requirements when renewing a valid certificate. Subjects who may have been unable to autoenroll for the initial certificate may be able to use autoenrollment to renew that certificate.
- On the **General** tab of the selected certificate template, the **Validity period** and **Renewal period** settings specify the valid lifetime of the certificate and how long before the end of its lifetime autoenrollment will request a renewal. Because the validity period can be very short and the renewal period may overlap, autoenrollment will not renew a certificate until at least 20% of the certificate lifetime has expired. This prevents autoenrollment from endlessly renewing a certificate due to misconfigured validity and renewal period settings.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Issuing Certificates from Pending Requests

To issue a certificate based on a certificate request:

1. Log on to the computer as a Certificate Manager.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node and select the **Pending Requests** folder. Requested certificates that are pending issuance will be displayed in the details pane.
4. Right-click on a request, point to **All Tasks** and then select **Issue**.

Deny a Certificate that is Pending Requests

To deny a certificate request:

1. Log on to the computer as a Certificate Manager.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node and select the **Pending Requests** folder. Requested certificates that are pending issuance will be displayed in the details pane.
4. Right-click the request, point to **All Tasks** and then select **Deny**.

Note: The policy module will always re-process requests that are pending and if template, configuration, or user group information has changed after the request was originally submitted, the policy module will re-evaluate the request based on the new information only.

Certificate Profile Management

Certificate profiles are maintained in the form of templates, which are an integral part of an enterprise CA. They are an important element of the certificate policy for an environment, which is the set of rules and formats for certificate enrollment, use, and management.

When a CA receives a request for a certificate, groups of rules and settings must be applied to that request to perform the requested function, such as certificate issuance or renewal. These rules can be simple or complex and may apply to all users or specific groups of users. Certificate templates are the sets of rules and settings that are configured on a CA to be applied against incoming certificate requests. Certificate templates also give instructions to the client on how to create and submit a valid certificate request.

Although all issued certificates are based on a certificate template, certificate templates can only be issued by an enterprise CA running on Microsoft Windows Server 2003, Enterprise Edition. The templates are stored in Active Directory for use by every CA in the forest. This allows the CA to always have access to the current standard template and ensures homogenous application of certificate policy across the Windows forest[8].

[8] A forest is a collection of one or more Windows Active Directory trees, organized as peers and connected by two-way transitive trust relationships between the root domains of each tree. All trees in a forest share a common schema, configuration, and Global Catalog. When a forest contains multiple trees, the trees do not form a contiguous namespace.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: Within the TOE, only an Enterprise CA may be used as an issuing CA. Stand-alone CAs may be used as offline root CAs, but are not included in the TOE.

The Certificate Server uses standard certificate templates to process certificate requests and issue certificates. It ensures that the certificates issued are consistent with the currently selected template. Certificate templates are stored as directory objects in the Active Directory in the IT Environment. A default set of templates is assigned to each Certificate Server when it is created, and the template selection may be modified by the CA Administrator through the **Certificate Templates** interface (certtmpl.msc snap-in). Certificates issued by a Certificate Server must conform to one of its assigned templates.

The Windows Server 2003, Enterprise Edition Certificate Server supports two basic types of certificate templates: version 1 and version 2. The version 1 templates are predefined and cannot be modified by the CA Administrator. Version 1 templates are provided for backwards compatibility with Windows 2000 Certificate Server and support many general needs for subject certification. They are created by default when a certification authority is installed and cannot be modified or removed. They can be duplicated, however, thereby creating a version 2 template that can be modified. Version 2 templates allow customization of various settings in the template. Preconfigured version 2 templates are supplied in the default configuration, and others can be added as necessary.

When deploying a Windows Server 2003 family enterprise CA, certificate templates are stored in Active Directory. This centralizes their location for use by all CAs in the enterprise and simplifies replication and security management. This also allows the CA to upgrade current certificate templates in Active Directory during installation.

Once the appropriate certificate templates are created, they will be replicated automatically to all Domain Controllers in the enterprise. This replication normally takes approximately eight hours to complete. Because of this interval, the certificate template should be created and allowed to replicate before deploying it to clients. This is best accomplished during an idle time in the environment. Configuring and using certificates before replication is completed can have unwanted effects.

The CA Administrator has the option of performing any of the following general certificate profile management tasks:

- View certificate template properties
- Create a new certificate template
- Modify certificate template permissions and ownership
- Delete a certificate template
- Add a certificate template to a CA
- Remove a certificate template from a CA
- Allow subjects to request a certificate based on a template
- Re-enroll all certificate holders
- Modify certificate template Properties

Each of these tasks is described below.

View Certificate Template Properties

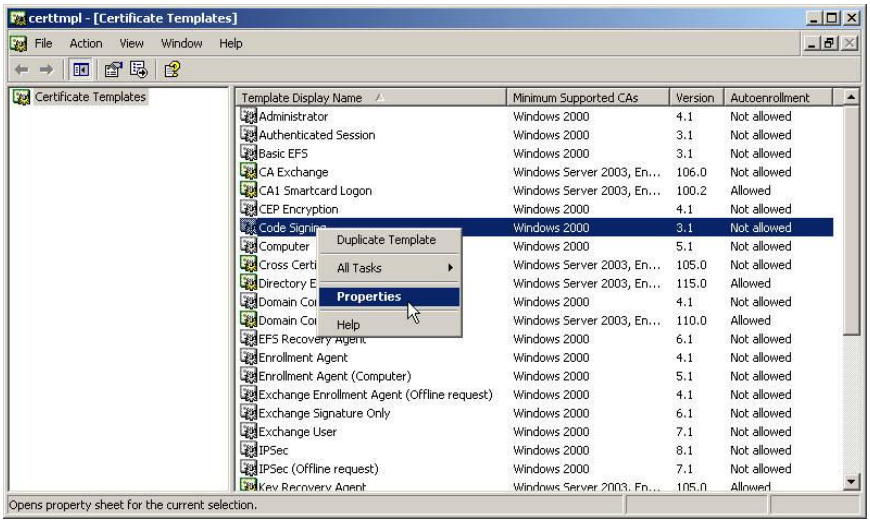
The properties of a certificate template can be viewed using the following procedure:

1. Log on to the computer as a CA Administrator.

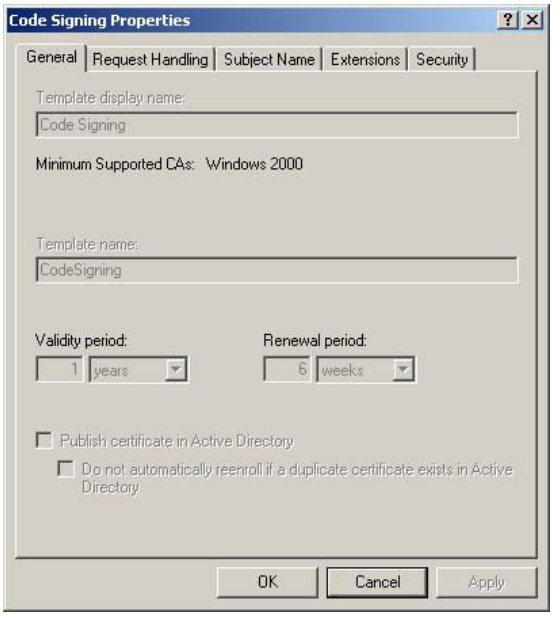
Copyright © 2008 Microsoft Corporation.

All rights reserved.

2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node, right click on the **Certificate Templates** folder and select **Manage**. The **Certificate Templates** interface will appear.
4. To view the properties for a certificate template right click on the certificate template in the details pane and select **Properties**.



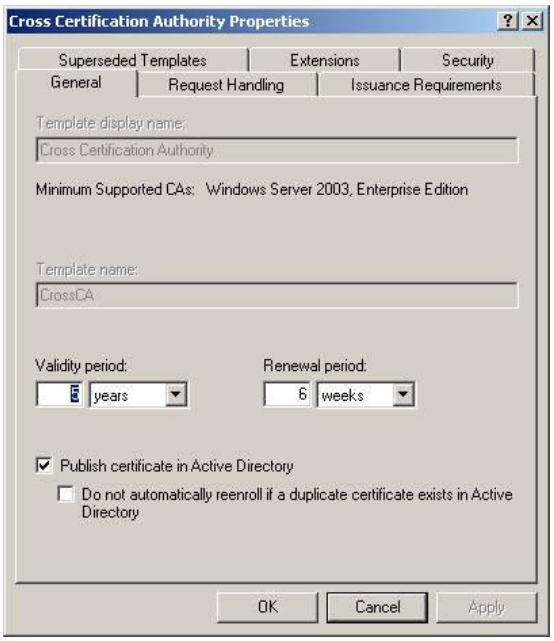
- When viewing a version 1 template, the following **Properties** interface is displayed:



- When viewing a version 2 template, the following **Properties** interface is displayed:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

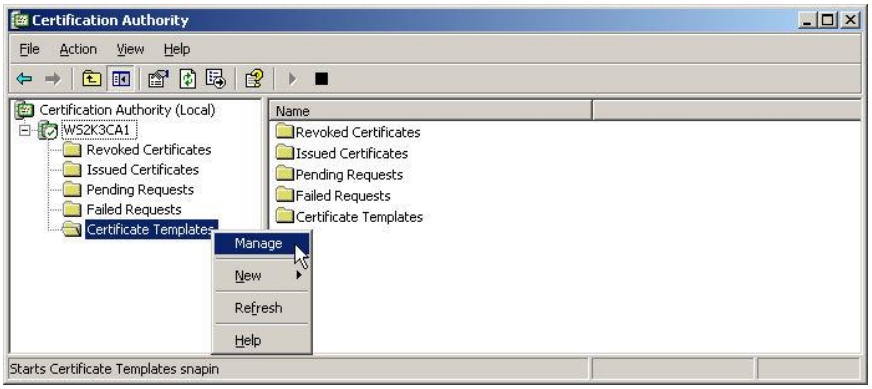


Create a New Certificate Template

New certificate templates must be created by duplicating an existing template and using the existing template's properties as a default starting point for the new template. Copy the existing certificate template closest to the configuration desired for the new template to minimize the work necessary to create it. All duplicates are created as version 2 templates.

To create duplicate certificate templates:

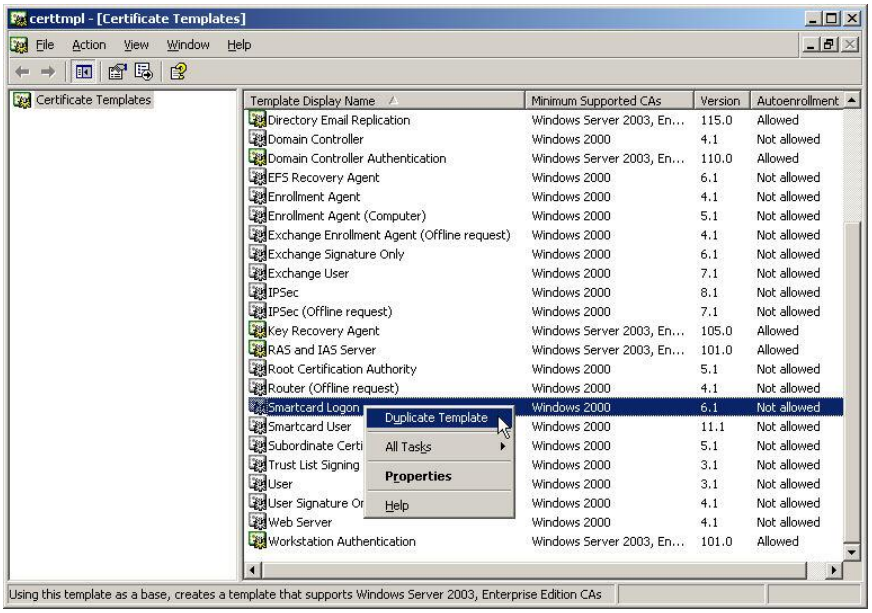
1. Log on to the computer as a Domain or Enterprise Administrator.
2. Open the **Certification Authority** interface. Click **Start**, point to **Administrative Tools**, and select **Certification Authority**. The **Certification Authority** interface will appear.
3. Expand the CA node, then right-click on the **Certificate Template** folder and select **Manage**.



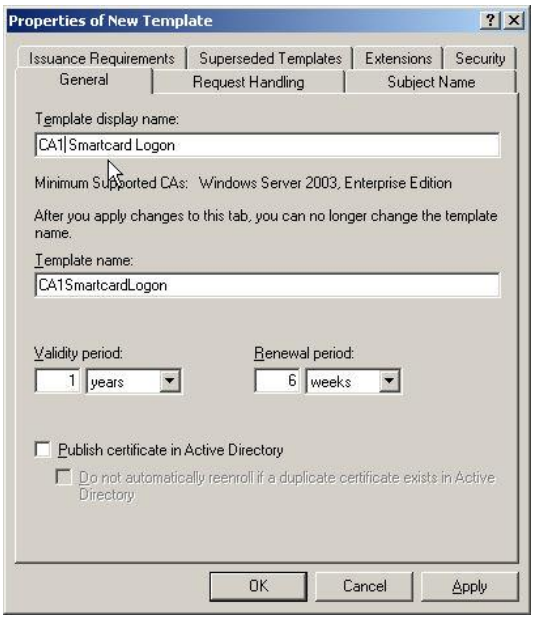
4. The **Certificate Templates** interface will appear. On the right-hand details pane, right-click on a template that is to be duplicated and select **Duplicate Template**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. A **Properties of New Template** interface will appear. Make appropriate changes to the template display name. Do not make other changes to the duplicate template at this time. Click **OK** to close the template.



6. The new duplicate template will appear in the right-hand details pane of the **Certificate Templates** interface with its new name. Further details for editing a certificate template are provided below in the Modification of Certificate Fields subsection.

Modify Template Permissions and Ownership

In order to modify certificate templates, the CA Administrator role will need both access permissions to the templates and ownership of the templates. Although permission and ownership changes can be made to the default templates, the ownership will revert back to Enterprise Admins whenever the templates interface is accessed by an Enterprise Administrator. To prevent this from occurring, it is necessary to

Copyright © 2008 Microsoft Corporation.

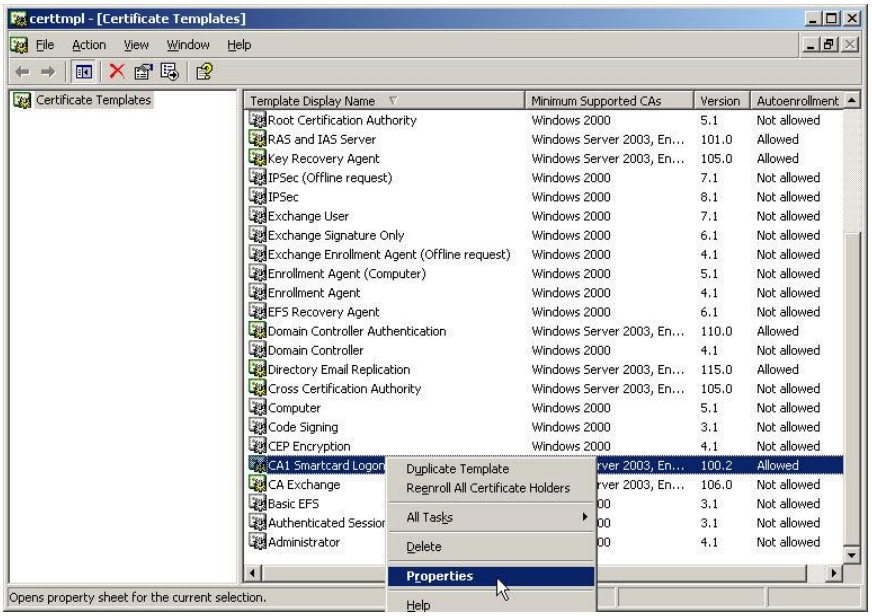
All rights reserved.

make duplicates of all the certificate templates that will be managed by the CA Administrator and then set the permissions and ownership as required. The ownership of duplicate templates will not change when accessed with domain or enterprise level administrative rights.

Additionally, to allow users to make certificate requests, they must be given the **Read** and **Enroll** permissions. Within the TOE, this is accomplished by giving the **Authenticated Users** group the **Read** and **Enroll** permissions. On version 2 templates there is an additional permission option to allow autoenrollment. To allow autoenrollment for a certificate, the security principle must be granted the **Read**, **Enroll**, and **Autoenroll** permissions.

To modify permissions and ownership on certificate templates:

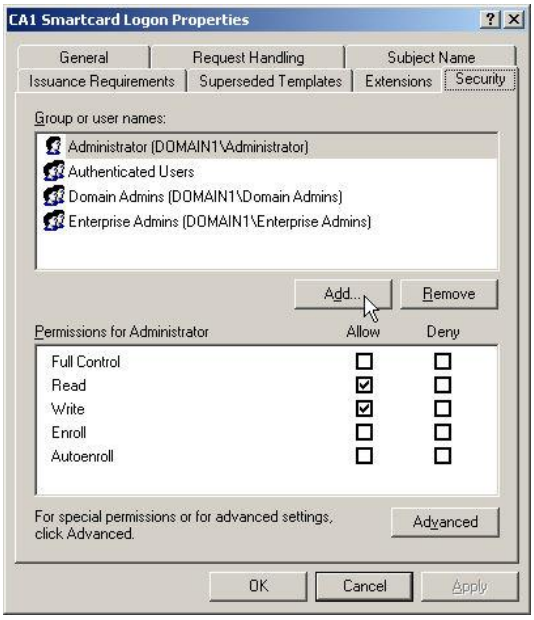
1. Log on to the computer as a Domain or Enterprise Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node, right click on the **Certificate Templates** folder and select **Manage**. The **Certificate Templates** interface will appear.
4. In the details pane of the **Certificate Templates** interface, right-click on a certificate template and select **Properties**.



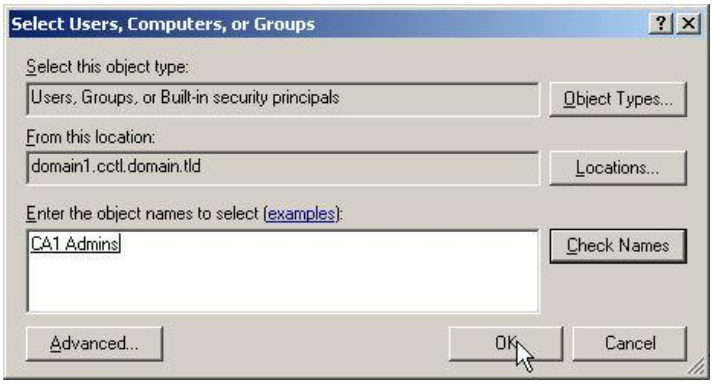
5. The **Properties** interface for the certificate template will appear. Select the **Security** tab to bring it to the foreground. To add permissions for the CA Administrator click the **Add** button.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



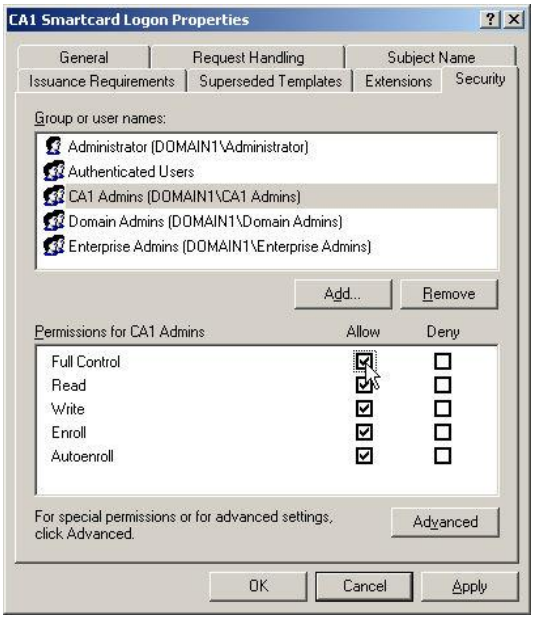
6. The **Select Users, Computers, or Groups** interface will appear. Enter the name of the group account that is designated for the CA Administrator role. If necessary, click the **Check Names** button to verify that the account exists. Click **OK**.



7. The account will appear in the **Group or user names** box. Highlight the account by selecting it. In the **Permissions for <user name>** window, check the **Allow** box for the **Full Control**. The remaining permission boxes will be automatically checked.

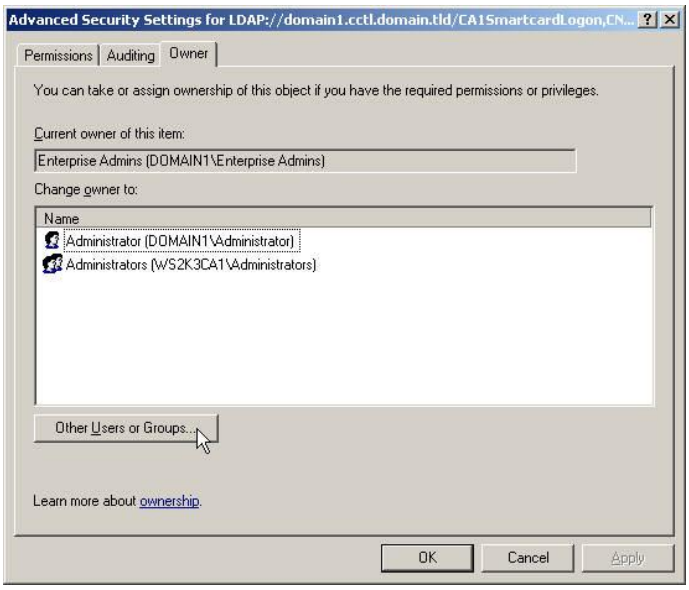
Copyright © 2008 Microsoft Corporation.

All rights reserved.



8. To modify permissions for the **Authenticated Users** group, select the group and check the **Allow** box for the permission that is to be granted. For example, check the **Read** and **Enroll** permission boxes.

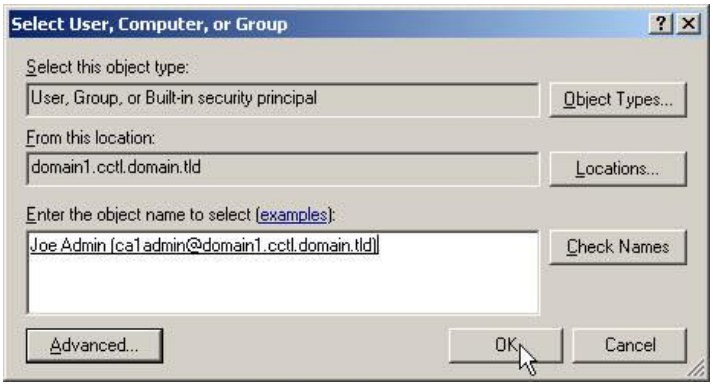
9. Click the **Advanced** button on the **Properties** interface. The **Advanced Security Settings** interface for the certificate template will appear. Select the **Owner** tab to bring it to the foreground.



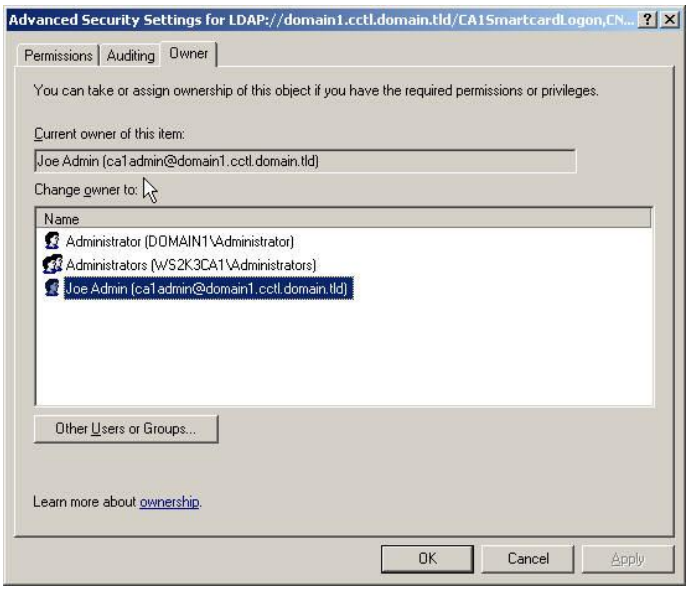
10. Click on the **Other Users or Groups** button. The **Select Users, Computers, or Groups** interface will appear. Enter the name of the "user" account that is designated for the CA Administrator role. If necessary, click the **Check Names** button to verify that the account exists. Click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



11. The account will appear in the **Change owner to** dialog box. Select the account assigned to the CA Administrator role from the **Change owner to** dialog box and click the **Apply** button. The account name will appear in the **Current owner of this item** dialog box.



12. Click **OK** to close the **Advanced Security Settings** interface for the certificate template.
13. Click **OK** on the **Properties** interface for the certificate template.

Deleting a certificate template

To permanently delete a certificate template:

1. Log on to the computer as a Domain or Enterprise Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node, right click on the **Certificate Templates** folder and select **Manage**. The **Certificate Templates** interface will appear.
4. In the details pane of the **Certificate Templates** interface, right-click on a certificate template and select **Delete**. A message will appear asking to confirm the deletion. Click **Yes**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

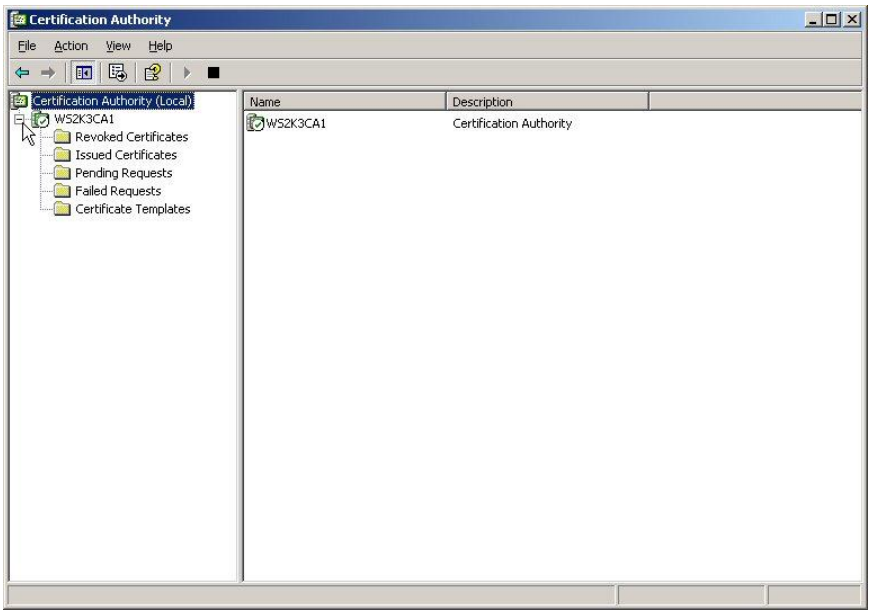
5. The certificate template will be deleted from the **Certificate Templates** interface and Active Directory.

Warning: When a certificate template is deleted, certificates can no longer be issued based on it. If Enterprise CAs are being used, this will affect all CAs in the forest. Certificate templates cannot be recovered once they are deleted.

Adding certificate templates to the CA for issuance

To include a certificate template in the list of certificates available for issuance by the CA:

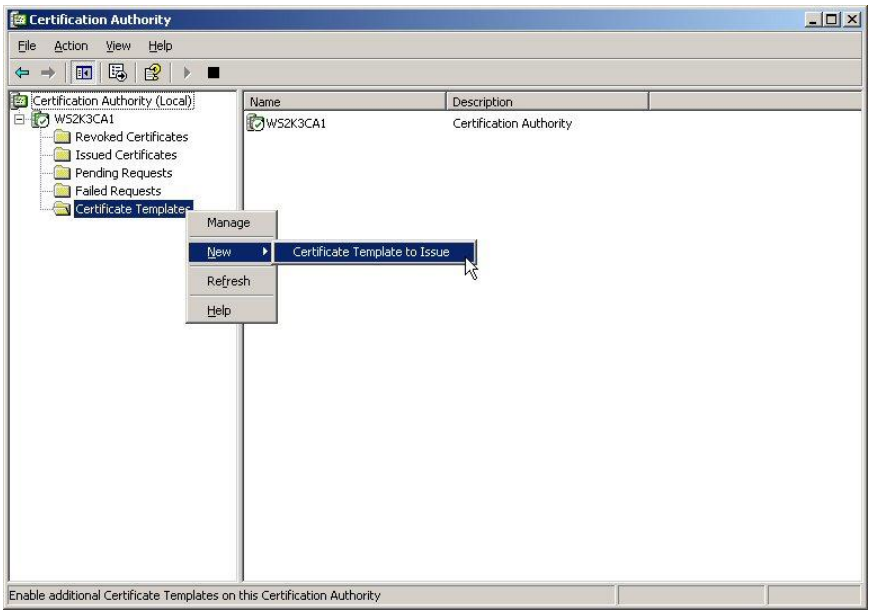
1. Log on to the computer as the CA Administrator.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node to view the **Certificate Templates** folder.



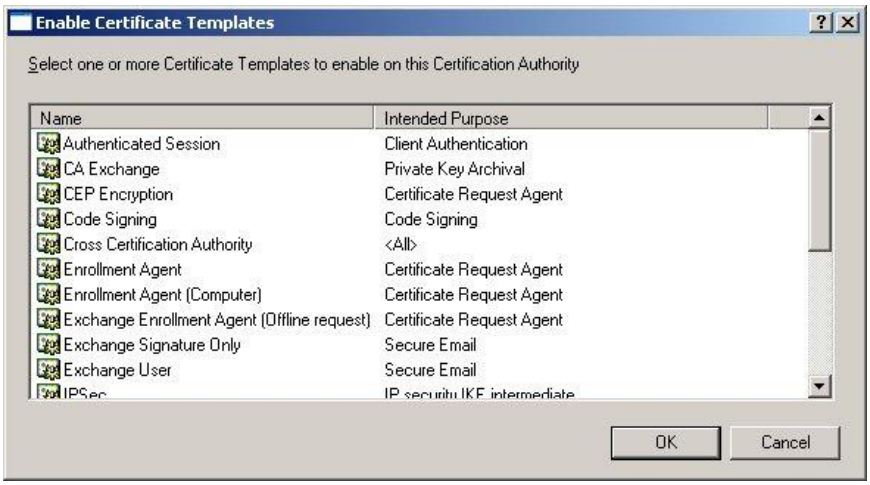
4. Right-click the **Certificate Templates** folder, select **New**, then select **Certificate Template to Issue**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



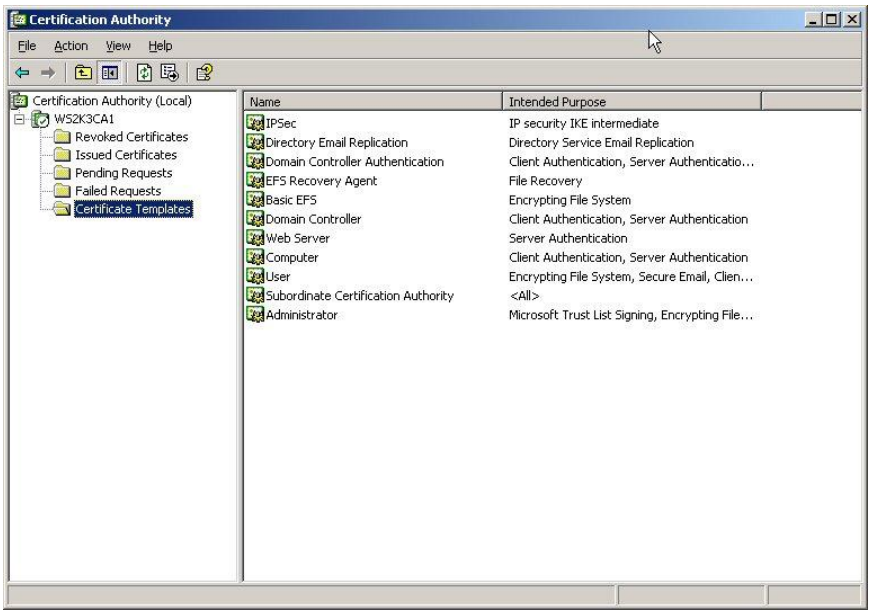
5. The **Enable Certificate Templates** interface will appear.



6. Select the template to add for issuance and click the **OK** button.
7. Select the **Certificate Templates** folder in the **Certification Authority** interface to verify that the added template appears in the list of templates in the right-hand details pane.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Removing certificate templates from the CA

To prevent a certificate from being issued by a CA:

1. Log on to the computer as the CA Administrator.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node to view the **Certificate Templates** folder.
4. Select the **Certificate Templates** folder, then right click on the certificate template that is to be removed from the right-hand details pane and select **Delete**.
5. The certificate template will be removed from the CA and can no longer be issued.

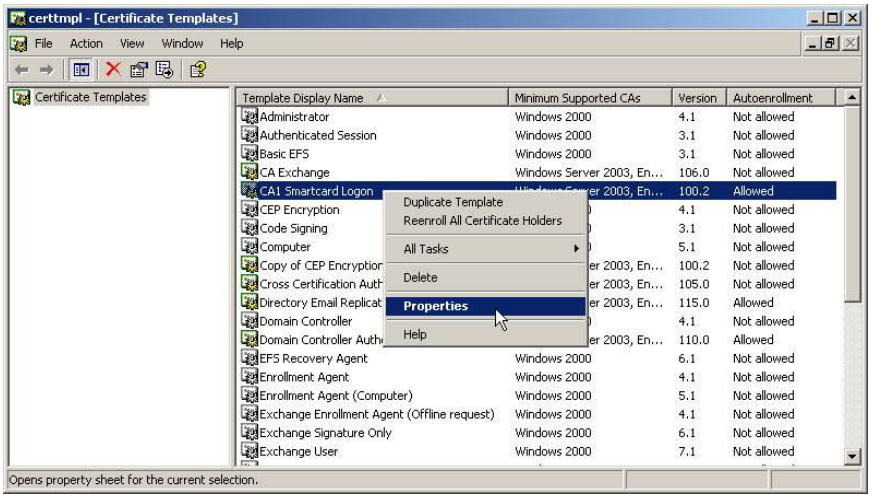
Allow subjects to request a certificate based on a template

As stated earlier, to request a certificate, users must have **Read** and **Enroll** permissions for the template on which the certificate is based. If the users do not have these permissions, the certificate will not be accessible to users via the **Certificate Request Wizard**. Use the procedures that follow to verify or set permissions and ensure that the **Authenticated Users** group or other specific user or group account has the ability to request certificates.

1. Log on to the computer as the CA Administrator.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node, right click on the **Certificate Templates** folder and select **Manage**. The **Certificate Templates** interface will appear.
4. In the details pane of the **Certificate Templates** interface, right-click the certificate template and select **Properties**.

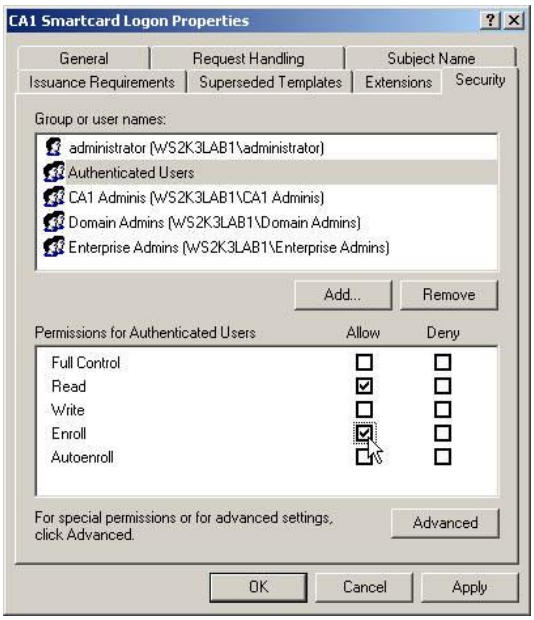
Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. Click the **Security** tab to view the permissions for the certificate. Select the user or group account for which permissions are to be verified or changed. If the group is not shown in the **Group or user names** list, click the Add button to add the group to the list.

6. In **Permissions for <ObjectName>**, under the **Allow** column, verify that the **Read** and **Enroll** permissions are assigned to the group. If not already assigned, select the **Read** and **Enroll** check boxes.



7. Add the template to the CA so it will be visible and available for issuance to users.

Re-enroll all certificate holders

If a critical change is made to a certificate template it may be necessary to ensure that all subjects that hold a certificate that is based on the template are re-enrolled as quickly as possible. To re-enroll all certificate holders for a specific certificate:

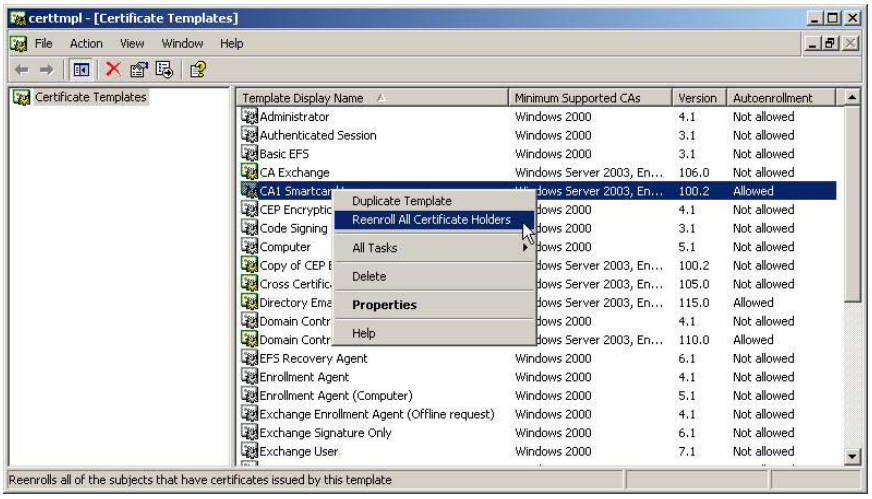
1. Log on to the computer as the CA Administrator.

2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. Expand the CA node, right click on the **Certificate Templates** folder and select **Manage**. The **Certificate Templates** interface will appear.
4. In the details pane of the **Certificate Templates** interface, right-click the certificate template and select **Reenroll All Certificate Holders**.



5. The next time the subject verifies the version of the certificate against the version of the template on the certification authority, the subject will re-enroll.

Modification of Certificate Fields

In the day-to-day management of the Certificate Server, there will be times when a CA Administrator must create a new certificate template or modify an existing certificate template. As shown in Table B-8, a variety of version 1 and version 2 certificate templates are available for different types of security applications. When a duplicate certificate template is made from a version 1 template, the duplicate will be a version 2 template.

Table B-8 Default Certificate Templates

Name	Description	Key Usage	Subject Type	Published to Active Directory?	Template Version
Administrator	Allows trust list signing and user authentication	Signature and encryption	User	Yes	1
Authenticated Session	Allows subject to authenticate to a Web server	Signature	User	No	1
Basic EFS	Used by Encrypting File System (EFS) to encrypt data	Encryption	User	Yes	1
CA Exchange	Used to store keys that are configured for private key archival	Encryption	Computer	No	2
CEP Encryption	Allows the holder to act as a registration authority (RA) for simple certificate enrollment protocol (SCEP) requests	Encryption	Computer	No	1

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Name	Description	Key Usage	Subject Type	Published to Active Directory?	Template Version
Code Signing	Used to digitally sign software	Signature	User	No	1
Computer	Allows a computer to authenticate itself on the network	Signature and encryption	Computer	No	1
Cross-Certification Authority	Used for cross-certification and qualified subordination.	Signature	CrossCA	Yes	2
Directory E-mail Replication	Used to replicate e-mail within Active Directory	Signature and encryption	DirEmailRep	Yes	2
Domain Controller	All-purpose certificates used by domain controllers	Signature and encryption	DirEmailRep	Yes	1
Domain Controller Authentication	Used to authenticate Active Directory computers and users	Signature and encryption	Computer	No	2
EFS Recovery Agent	Allows the subject to decrypt files previously encrypted with EFS	Encryption	User	No	1
Enrollment Agent	Used to request certificates on behalf of another subject	Signature	User	No	1
Enrollment Agent (Computer)	Used to request certificates on behalf of another computer subject	Signature	Computer	No	1
Exchange Enrollment Agent (Offline request)	Used to request certificates on behalf of another subject and supply the subject name in the request	Signature	User	No	1
Exchange Signature Only	Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for digitally signing e-mail	Signature	User	No	1
Exchange User	Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for encrypting email	Encryption	User	Yes	1
IPSEC	Used by IP Security (IPSec) to digitally sign, encrypt, and decrypt network communication	Signature and encryption	Computer	No	1
IPSEC (Offline request)	Used by IP Security (IPSec) to digitally sign, encrypt and decrypt network communication when the subject name is supplied in the request	Signature and encryption	Computer	No	1

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Name	Description	Key Usage	Subject Type	Published to Active Directory?	Template Version
Key Recovery Agent	Recovers private keys that are archived on the certification authority.	Encryption	KRA	No	2
RAS and IAS Server	Enables RAS and IAS servers to authenticate their identity to other computers	Signature and Encryption	Computer	No	2
Root Certification Authority	Used to prove the identity of the root certification authority	Signature	CA	No	1
Router (Offline request)	Used by a router when requested through Simple Certificate Enrollment Protocol (SCEP) from a certification authority that holds a CEP Encryption certificate	Signature and encryption	Computer	No	1
Smartcard Logon	Allows the holder to authenticate using a smart card	Signature and encryption	User	No	1
Smartcard User	Allows the holder to authenticate and protect e-mail using a smart card	Signature and encryption	User	Yes	1
Subordinate Certification Authority	Used to prove the identity of the root certification authority. It is issued by the parent or root certification authority	Signature	CA	No	1
Trust List Signing	Allows the holder to digitally sign a trust list	Signature	User	No	1
User	Used by users for e-mail, EFS and client authentication	Signature and encryption	User	Yes	1
User Signature Only	Allows users to digitally sign data	Signature	User	No	1
Web Server	Proves the identity of a Web server	Signature and encryption	Computer	No	1
Workstation Authentication	Enables client computers to authenticate their identity to servers	Signature and encryption	Computer		

Copyright © 2008 Microsoft Corporation.

All rights reserved.

The specific version 1 or version 2 certificate template selected governs which fields will be present in a certificate9 and for version 2 which fields have modifiable settings. The material that follows describes how the CA Administrator can configure these certificate templates to select specific values.

To modify settings for a certificate template:

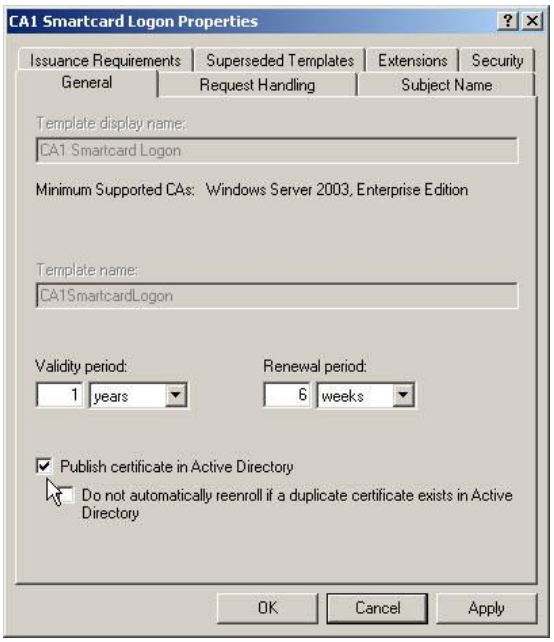
1. Log on to the computer as a CA Administrator.
2. Click **Start**, select **All Programs**, select **Administrative Tools**, and select **Certification Authority**.
3. Expand the CA node, right click on the **Certificate Templates** folder and select **Manage**.
4. In the details pane, right-click the certificate template to be modified, and then select **Properties**.
5. Click the desired tab and then modify the settings as needed.

Descriptions for configurable certificate template settings are provided in the subsections below.

Note: The issuer name is established during the installation of the CA and cannot be modified by the CA Administrator.

General settings: Modify validity and renewal periods

Some version 2 certificate templates allow the CA Administrator to specify the validity period and renewal periods for certificates based on the template. The validity and renewal periods can be modified from the General tab view of the certificate template. Other settings that can be modified from the General tab view include the option of publishing certificates in Active Directory, automatic reenrollment if a duplicate exists, and the template name.



The following settings can be configured from the **General** tab view of a version 2 certificate template:

9 Some fields must always be present such as Version, Certificate Serial Number, Signature Algorithm Identifier, Issuer Name, Period of Validity, Subject name, and Subject's Public Key information.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

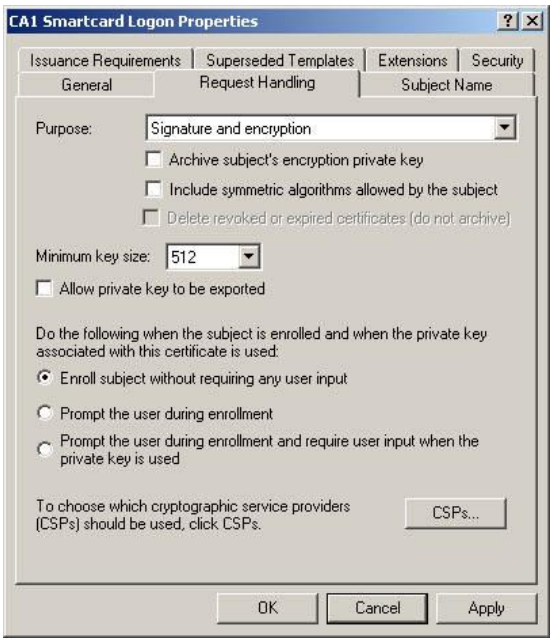
- **Template display name**. The display name shown in the **Certificate Templates** interface, **Certificates** interface, and in the **Certification Authority** interface.
- **Template name** The name of the certificate template object created in the CN=Certificate Templates,CN=Public Key Services,CN=Services,DC=*ForestRootDomain* container.

Note: The template display name and template name attributes can only be modified when a template is being created (by making a duplicate template) and cannot be changed once the certificate template is created.

- **Validity period**. Defines the validity period for an issued certificate. The validity period must not be defined to be greater than the validity period of the CA's certificate.
- **Renewal period**. The time before the validity period expires when the certificate will be renewed if re-enrollment is supported for the certificate template. The minimum renewal period is 80% of the certificate lifetime or 6 weeks, whichever is greater.
- **Publish certificate in Active Directory**. Allows the option to publish the certificate to Active Directory based on the certificate template. The certificates are published as an attribute of the security principal contained in the subject of the issued certificate.
- **Do not automatically reenroll if a duplicate certificate exists in Active Directory**. If the certificate template is published to Active Directory, this option can be used to prevent re-enrollment if a valid certificate of the same certificate template exists for the security principal indicated in the subject.

Request handling

The Request Handling tab defines the purpose of the certificate template, the supported cryptographic service providers (CSPs), minimum key length, exportability, auto-enrollment settings, and whether strong private key protection should be required.



The following settings can be configured from the General tab view of a version 2 certificate template:

- Certificate **Purpose**. The certificate purpose defines the intended primary use of the certificate. The certificate purpose can be one of four settings that can be selected from the Purpose pull-down menu:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Encryption**. A certificate with this purpose will contain cryptographic keys for encryption and decryption.
- **Signature**. A certificate with this purpose will contain cryptographic keys for signing data only.
- **Signature and encryption**. A certificate with this purpose covers all primary uses of a certificate's cryptographic key, including encryption of data, decryption of data, initial logon, or digitally signing data.
- **Signature and smartcard logon**. A certificate with this purpose allows for initial logon with a smart card, and to digitally sign data; it cannot be used for data encryption.

Note: The certificate purpose setting will determine whether key archival can be enabled for a certificate template. Key archival is only possible if the certificate purpose is set to Encryption or Signature and encryption. The recovery of a private key for digitally signing information may result in identity theft and is not supported. Key archival is not supported by most smart card CSPs.

- **Archive Settings**. When subjects lose their private keys due to user profile corruption or stolen computers, any information that was persistently encrypted with the corresponding public key is inaccessible. To help avoid this, Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition have the ability to archive a subject's keys in its database when certificates are issued. These keys are encrypted and stored by the CA. If subjects lose their keys, the information can be retrieved from the database and securely provided to the subjects. This allows the encrypted information to be recovered instead of lost. The following Key Archival settings are defined in the **Request Handling** tab:
  - **Archive subject's encryption private key**. If the issuing Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition certification authority is configured for key archival, the subject's private key will be archived.
  - **Include symmetric algorithms allowed by the subject**. When subjects request the certificate, they can supply a list of supported symmetric algorithms. This option allows the issuing certification authority to include those algorithms in the certificate, even if they are not recognized or supported by that server. The algorithms are used by applications like secure e-mail.
  - **Delete revoked or expired certificates (do not archive)**. If a certificate is renewed due to expiration or revocation, the previously issued certificate is removed from the subject's certificate store. By default, the certificate is archived.
  - **Allow private key to be exported**. When this option is specified, the subject's private key can be exported for backup or transportation.

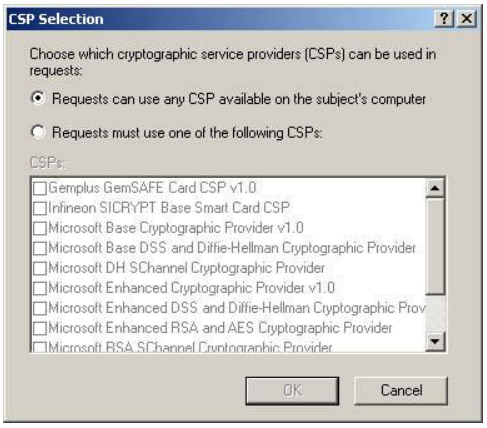
  To enable key archival and recovery, the following configuration settings in the certificate template and at the Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition CA must be made:
  - The specific certificate template must be configured to allow key archival.
  - One or more key recovery agents must be identified on the certification authority and key recovery agent certificates must be issued to those agents.
  - Key archival must be configured on the CA.
- **Minimum key size**. This specifies the minimum size, in bits, of the key that will be generated for this certificate.
- **User Input Settings**. The **Request Handling** tab also allows several user input settings to be defined for a certificate template. These settings include:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **Enroll subject without requiring any user input**. This option allows auto-enrollment without any user interaction and is the default setting for both machine and user certificates. This option must not be enabled for machine certificates.
- **Prompt the user during enrollment**. Although useful when testing initial auto-enrollment deployments, typically, this option is disabled. By disabling this option, users do not have to provide any input for the installation of a certificate based on the certificate template.
- **Prompt the user during enrollment and require user input when the private key is used**. This option enables the user to set a strong private key protection password on the user's private key when the key is generated and requires the user to use it whenever the certificate and private key are used. This option must not be enabled for machine certificates or smart card user certificates.

- **CSPs**. This is a list of CSPs that will be used to enroll certificates for the given template. Selecting one or more CSPs configures the certificate to only work with those CSPs. If a specific CSP is not selected, the certificate enrollment will work with any installed CSP, but will use the first CSP from the enumeration list. The CSP must be installed on the client workstation for the CSP to be used during enrollment. If a specific CSP is chosen and not available on a client machine, enrollment will fail. The CSP Selection interface can be accessed by clicking the **CSPs** button on the **Request Handling** tab view of the certificate template's **Properties** interface.

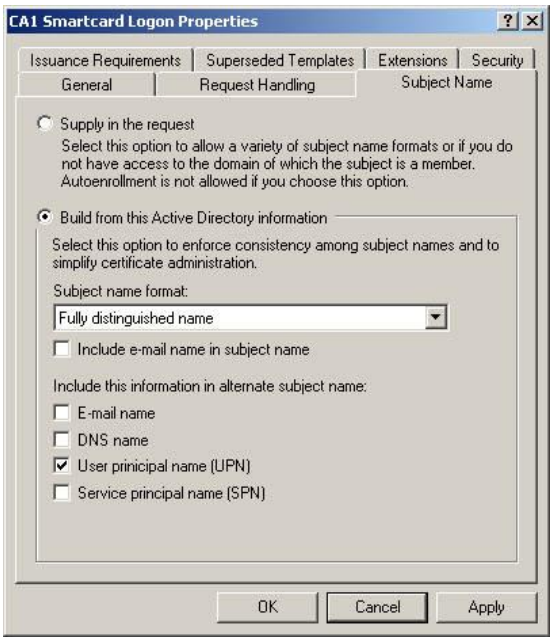


Subject Name

When establishing a certificate template, the subject name must be defined. This is included in the issued certificate template and must uniquely identify the subject. The subject name can either be built automatically during the certificate request or explicitly defined by the subject and included in the certificate request. Some version 2 certificate templates allow the CA Administrator to specify how to define the subject name.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



Following are options that can be included with the subject name, as well as specific configuration settings for the subject name:

- **Supply in the request**. If the **Subject Name** option is set to **Supply in the request**, one or more **Issuance Requirements** should be set for the template. If no **Issuance Requirements** are set, subjects may be able to request and obtain certificates that contain any subject name. This would allow subjects to impersonate other subjects easily. Issuance requirements ensure that the certificate request is inspected and validated before the certificate is issued.

  Note: No user interface exists on the client to supply a subject name in the certificate request. In Windows Server 2003 Certificate Server, the only case in which a subject can request a certificate with a different subject name is when the requestor holds a certificate based on the Enrollment Agent template. The Enrollment Agent template allows a subject to request a certificate on behalf of another subject.

- **Build from this Active Directory information**. A number of options can be included with the subject name, as well as specific configuration settings for the subject name when the subject name is built from Active Directory information during the certificate request process.
  - **Subject name format**. The format of the subject name can be defined as:
    - **Common name**. The certification authority creates the subject name from the common name (CN) obtained from Active Directory. These should be unique within a domain, but may not be unique within an enterprise.
    - **Fully distinguished name**. The certification authority creates the subject name from the fully distinguished name obtained from Active Directory. This guarantees that the name is unique within an enterprise.
    - **None**. Does not enforce any name format for this field.
  - **Include e-mail name in subject name**. If the e-mail name field is populated in the Active Directory user object, that e-mail name will be included with either the common name or fully distinguished name as part of the subject name.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Note: The e-mail name is required for user certificates. If the e-mail name is not populated for a user in Active Directory, the certificate request by that user will fail.

- **Include this information in the alternate subject name.** In addition to the subject name, name formats can be chosen for inclusion in the alternate subject name attributes of issued certificates. The alternate subject name formats are shown in Table B-9.

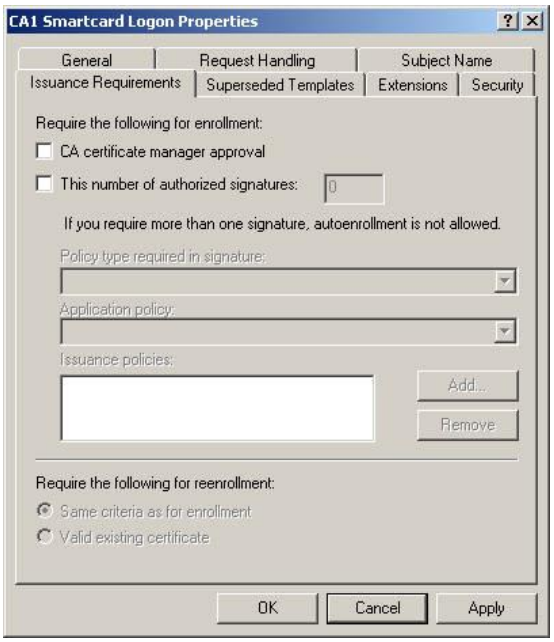
Table B-9 Alternate Subject Name Options

Field	Description	Useful for subject types
E-mail name	If the e-mail name field is populated in the Active Directory user object, that e-mail name will be used.	User
DNS name	The fully qualified domain name (FQDN) of the subject that requested the certificate.	Computer
User principal name (UPN)	The user principal name is part of the Active Directory user object and will be used.	User
Service principal name (SPN)	The service principal name is part of the Active Directory computer object and will be used.	Computer

Issuance Requirements

The Issuance Requirements tab (Figure 4) allows higher assurance level certificates to be placed in a pending state until the certificate is reviewed before issuance. This allows for multiple signers of a CMC (Certificate Management over Cryptographic Message Syntax (CMS)) request to exist.

Note: For information on CMC, see RFC 2797 Certificate Management Messages over CMS.



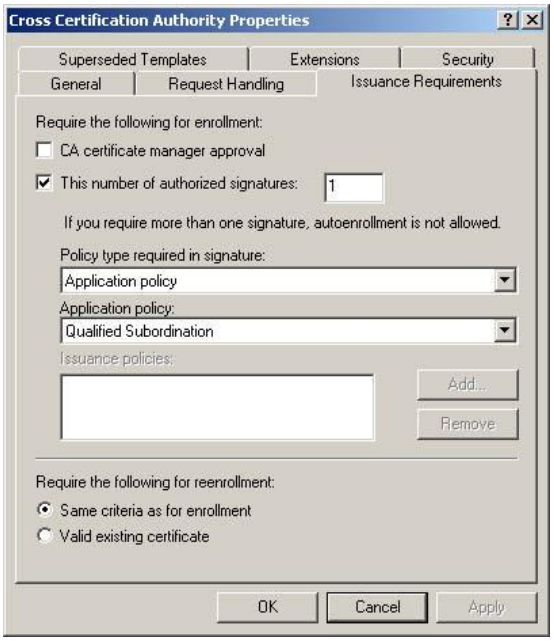
When CA certificate manager approval is enabled, the certificate is placed into a pending state, rather than being issued immediately. In its pending state, the certificate request can be reviewed by certificate managers, ensuring a higher level of assurance for the issued certificate. The following settings configure the authentication and signature requirements for issuance certificates that are based on a template:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- **CA certificate manager approval**. All certificates are placed into the pending container for a certificate manager to issue or deny. Any defined certificate manager can issue or deny a certificate request of this type.
- **This number of authorized signatures**. This setting requires the CMC certificate request to be digitally signed by one or more authorized parties before it can be issued. Defining the number of authorized signatures enables several other configuration parameters:
  - **Policy type required in signature**. This option defines which specific application policy, issuance policy, or both are required in the signing certificate. This is how the certification authority determines whether the signature is appropriate for authorizing the issuance of the subject's certificate.
  - **Application policy**. This option specifies the application policy that must be included in the signing certificate used to sign the certificate request. It is enabled when **Policy type required in signature** is set to either **Application policy** or both **Application** and **issuance policy**.
  - **Issuance policy**. This option specifies the issuance policy that must be included in the signing certificate used to sign the certificate request. This option is enabled when **Policy type required in signature** is set to either **Issuance policy** or both **Application** and **issuance policy**.

  An example of where issuance requirements are defined is for the issuance of **Cross-Certification Authority** certificates. This certificate template requires that the signing certificate includes the Qualified Subordination **Application Policy** object identifier (OID) as shown below. As shown, the Cross-Certification Authority certificate request must be signed by a certificate containing the **Qualified Subordination** OID.



- **Require the following for reenrollment**. Options are provided to determine whether the same issuance requirements are upheld for certificate renewal, or if the existence of a valid certificate of the same template in the certificate store meets the minimum requirements for certificate issuance.

Copyright © 2008 Microsoft Corporation.

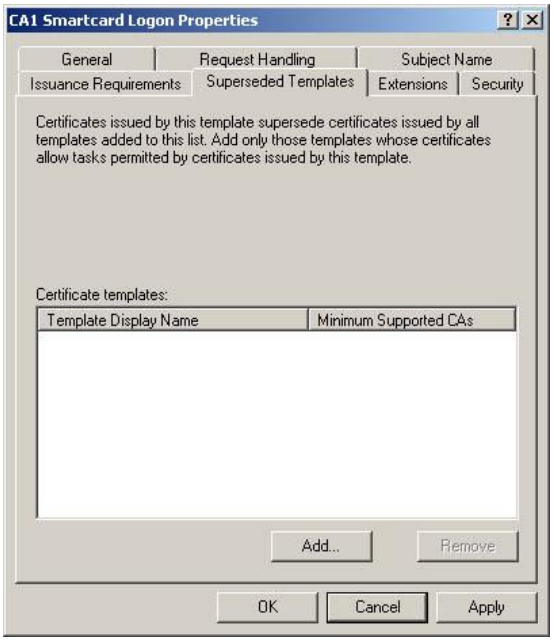
All rights reserved.

Superseded Templates

Certificate templates can be superseded. This procedure is used to replace one template with another. Subjects of certificates based on the old template should obtain new certificates based on the new template. This forces subjects to obtain a new certificate before their configured renewal period.

The **Superseded Templates** tab allows CA Administrators to redeploy version 2 certificates and ensure that the updated certificates replace previous versions of the certificate or other certificate templates that were used for the same purposes. The **Superseded Templates** tab can be used to supersede:

- A version 1 certificate template with a version 2 certificate template;
- A version 2 certificate template with a version 2 certificate template; and
- Multiple existing certificate templates with a common version 2 certificate template.



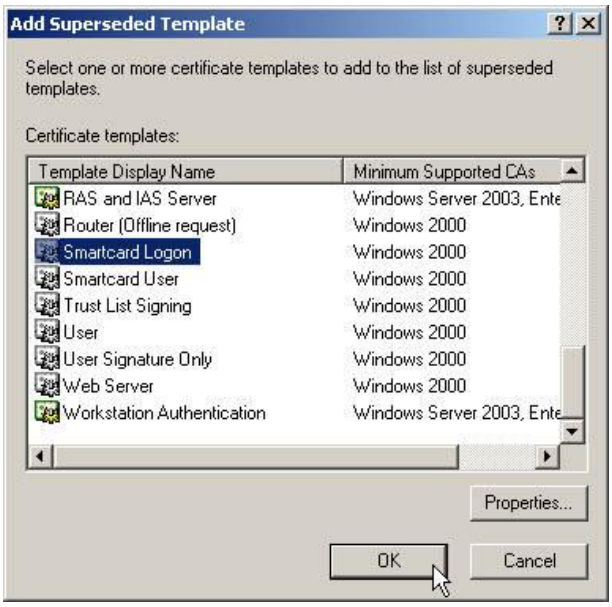
To supersede a template:

Note: This procedure is applicable to version 2 templates only.

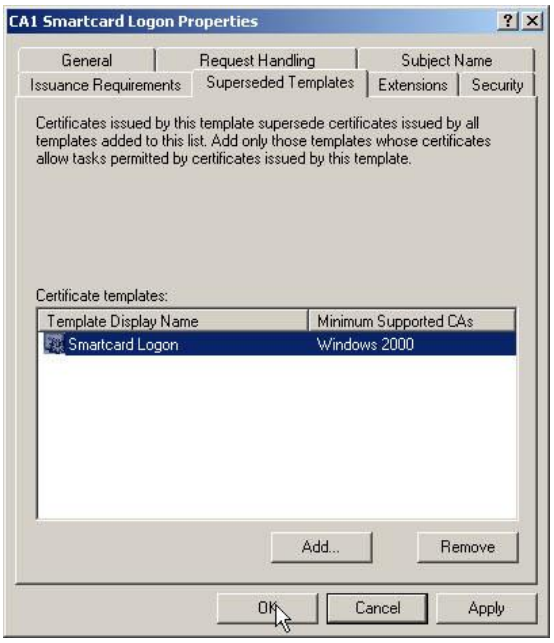
1. Click **Add** on **the Superseded Templates** tab view of the certificate template's **Properties** interface.
2. Click one or more templates to supersede, and then click **OK**.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



3. The superseded template will appear in the **Certificate templates** list box of the **Superseded Templates** tab view. Click **OK**.

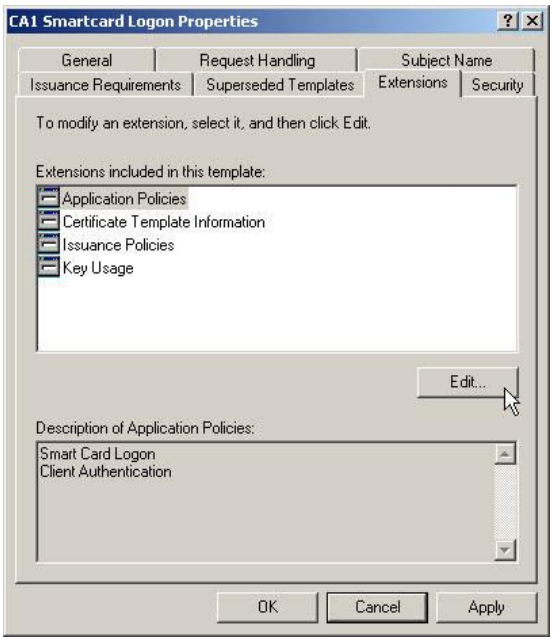


Extensions

The **Extensions** tab allows CA Administrators to define specific application policies, issuance policies, certificate subject types, and key usage attributes for a certificate template.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



The following are details on each form of extension defined in a certificate template.

- **Application Policies**. Application policies enable the CA Administrator to decide which certificates can be used for certain purposes. Application policies include settings that inform a target that the subject holds a certificate that can be used to perform a specific task. They are represented in a certificate by an OID that is defined for a given application. This object identifier is included in the issued certificate. When a subject presents its certificate, it can be examined by the relying party to verify the application policy and determine if it can perform the requested action. Table B-10 shows some of the more commonly used application policies and their related OIDs.

  Note: Application policies are similar to the *extended key usage* attribute in version 1 certificate templates. Because some implementations of PKI applications may not understand application policies, both application policies and enhanced key usage sections appear in certificates issued by a Microsoft CA.

Table B-10 Commonly Used Application Policies

Application Policy	OID
Client Authentication	1.3.6.1.5.5.7.3.2
CA Encryption Certificate	1.3.6.1.4.1.311.21.5
Smart Card Logon	1.3.6.1.4.1.311.20.2.2
Document Signing	1.3.6.1.4.1.311.10.3.12
File Recovery	1.3.6.1.4.1.311.10.3.4.1
Key Recovery	1.3.6.1.4.1.311.10.3.11
Microsoft Trust List Signing	1.3.6.1.4.1.311.10.3.1
Qualified Subordination	1.3.6.1.4.1.311.10.3.10
Root List Signer	1.3.6.1.4.1.311.10.3.9

Copyright © 2008 Microsoft Corporation.

All rights reserved.

An OID is a number that identifies an object class or attribute. OIDs are organized into an industry-wide global hierarchy. An object identifier is represented as a dotted decimal string, such as 1.2.3.4, with each dot representing a new branch in the hierarchy. National registration authorities issue root object identifiers to individuals or organizations, who manage the hierarchy below their root OID.

- **Certificate Template Information**. The certificate template information, also referred to as the Certificate subject type, defines the purpose of a certificate template. Six subject types are recognized by Windows Server 2003 CAs:
  - Key recovery agent
  - Directory e-mail replication
  - Cross-certified certification authority
  - Certification authority (CA)
  - Computer
  - User

  The certificate template information extension cannot be edited. If a specific subject type is required to be applied to a certificate, the CA Administrator should duplicate a certificate template that includes the required subject type. Some of the internal flags that are defined for specific subject types limit the display of the certificate template to computers or users. Choosing to duplicate an incorrect certificate template will prevent the certificate template from being displayed to the desired enrollment audience. For example, a computer certificate template cannot be enrolled for use by a user account.

- **Issuance Policies**. An issuance policy describes the conditions under which a certificate is issued. This provides a level of assurance that the subject's certificate request was verified in a specific way. One or more issuance policies may be selected for a certificate template. Because these issuance policies are simply text labels with an associated object identifier, there are no options associated with them. The only special issuance policy is the "All issuance policies," which indicates that this policy includes all others. This is normally reserved for certificates held by certification authorities.

  An issuance policy (also known as a certificate policy) is a group of administrative rules that is implemented when issuing certificates. These administrative rules are represented in a certificate by an object identifier (also known as an OID) that is defined at the certification authority. This object identifier is included in the issued certificate. When a subject presents its certificate, it can be examined by the target to verify the issuance policy and determine if that level of issuance policy is sufficient to perform the requested action.

- **Key Usage**. The Certificate Server establishes subject/public-key relationships when it issues certificates to subjects. The usage of these keys is configured by key usage and application policy. The key usage setting constrains the types of operations that can be performed with a certificate. There are several options (defined in Tables B-11 and B-12), depending on what purpose has been configured for this certificate: Signature, Encryption or both.

Note: Certificate Server does not generate key pairs for certificate subjects.

Table B-11 Signature Key Usage Settings

Setting	Description
Digital signature	Data can be digitally signed by this certificate. This is the most basic signature operation.
Signature is proof of origin (non-repudiation)	Data signed by this certificate can be traced back to the subject that provided the digital signature. This provides non-repudiation of signatures and is useful in certificate-based transactions.
Certificate signing	This certificate can be used to sign other certificates. This option is normally

Copyright © 2008 Microsoft Corporation.

All rights reserved.

	granted to certificate managers and certificates used by certification authorities.
CRL signing	This certificate can be used to sign CRLs. This option is normally granted to officers and certificates used by certification authorities.

Table B-12 Encryption Key Usage Settings

Setting	Description
Allow key exchange without key encryption (key agreement)	This option configures the subject to use a key agreement protocol, such as Diffie-Hellman, to establish a symmetric key that can be used to encrypt and decrypt data between the subject and the intended target.
Allow key exchange only with key encryption (key encipherment)	This option will configure the subject to establish a symmetric key with a target by generating a symmetric key, encrypting it, and sending it to the target for decryption.
Allow encryption of user data	With this option, the subject can use the established symmetric key to encrypt and decrypt actual application data with the same key used for key establishment. This option is only available when **Allow key exchange only with key encryption (key encipherment)** is selected.

A certificate enables the subject to perform a specific task. To help control the usage of a certificate outside its intended purpose, restrictions can be automatically placed on certificates. The **Key Usage** extension is a restriction method that determines how a certificate is used. This allows the CA Administrator to issue certificates that can only be used for specific tasks or certificates that can be used for a broad range of functions. Some version 2 certificate templates allow the CA Administrator to explicitly specify Key Usage values. The specific procedure for accomplishing this task is as follows:

- **Basic Constraints**. Certification authorities (CAs) must have a certificate before they can issue certificates. They use the private key associated with this certificate to digitally sign issued certificates. When a CA obtains a certificate from another CA, the parent CA may want to control whether that certificate can be used to issue certificates to other certificate servers. This is a basic constraint. Some version 2 certificate templates allow the CA Administrator to specify how the value of the Basic Constraints extension is selected. The specific procedure for accomplishing this is as follows:

To Add, Edit, or Remove an **Application Policy**:

1. Select the **Extensions** tab of the certificate template's **Properties** interface.
2. Select the **Application Policy** extension and click the **Edit** button. The **Edit Application Policies Extension** interface will appear.

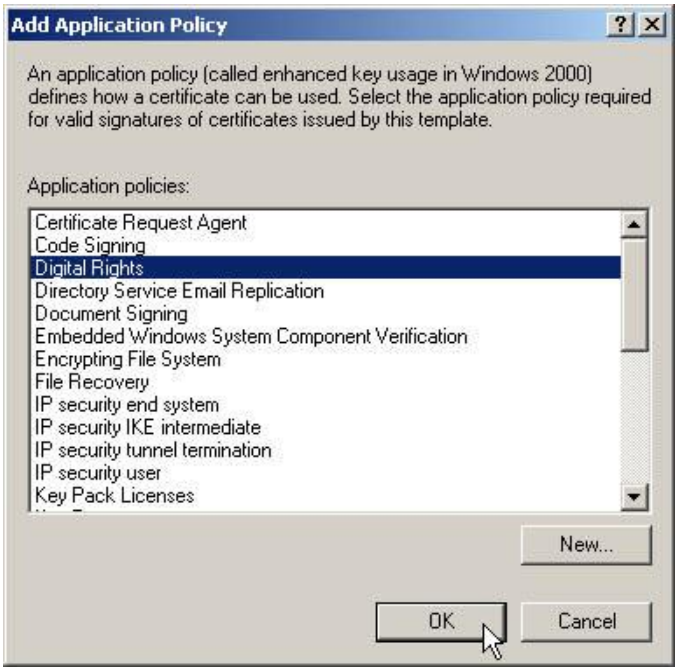
Copyright © 2008 Microsoft Corporation.

All rights reserved.

3. To edit an application policy, select it and click the **Edit** button. To remove an application policy, select it and click the **Remove** button.

Note: Most application policies will not be editable.

4. To add an application policy, click the **Add** button. The **Add Application Policy** interface will appear. Select the application policy to be added and click **OK**.



5. To create a new application policy, click the **New** button on the **Add Application Policy** interface and enter the appropriate information in the **New Application Policy** interface.

To Add, Edit, or Remove an **Issuance Policy**:

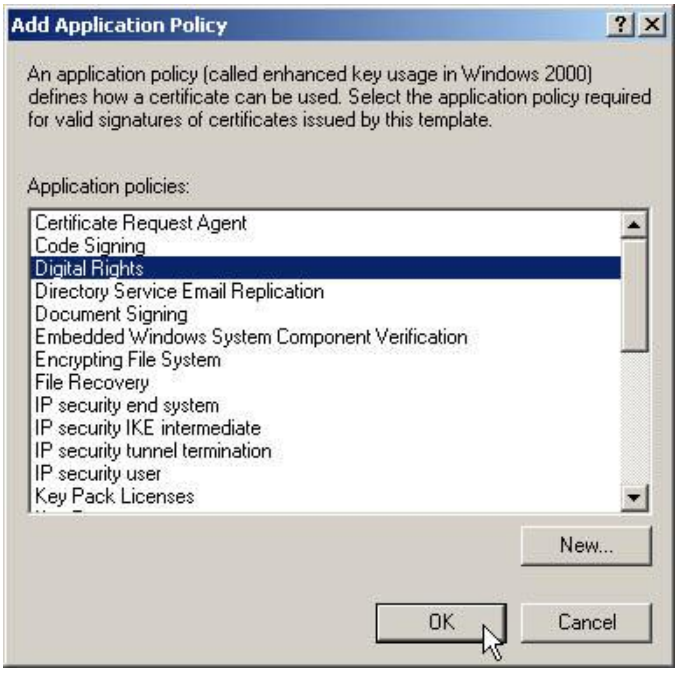
1. Select the **Extensions** tab of the certificate template's **Properties** interface.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

2. Select the **Issuance Policy** extension and click the **Edit** button. The **Edit Issuance Policies Extension** interface will appear.
3. To edit an issuance policy, select it and click the **Edit** button. To remove an issuance policy, select it and click the **Remove** button.

4. To add an issuance policy, click the **Add** button. The **Add Issuance Policy** interface will appear. Select the issuance policy to be added and click **OK**.



5. To create a new issuance policy, click the **New** button on the **Add Issuance Policy** interface and enter the appropriate information in the **New Issuance Policy** interface.

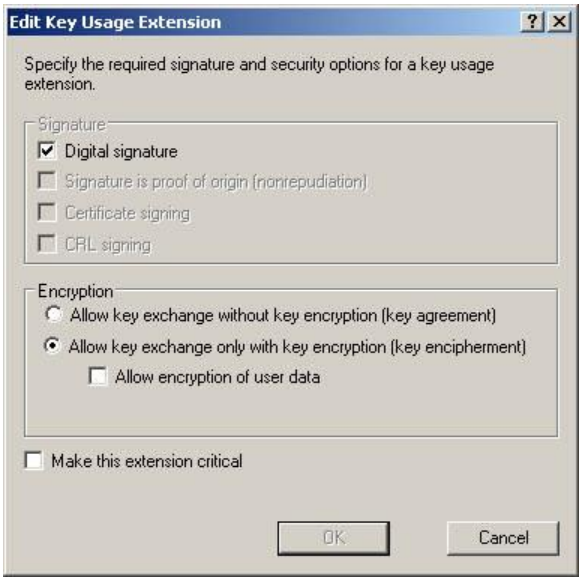
To Edit the **Key Usage** extension:

1. Select the Extensions tab of the certificate template's Properties interface.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

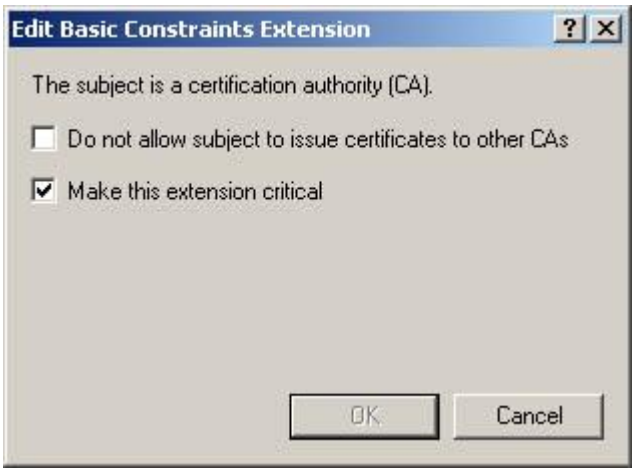
2. Select the Key Usage extension and click the Edit button. The Edit Key Usage Extension interface will appear.



3. Make any necessary changes and click OK.

To Edit the **Basic Constraints** extension:

1. Select the **Extensions** tab of the certificate template's **Properties** interface.
2. Select the **Basic Constraints** extension and click the **Edit** button. The E**dit Basic Constraints Extension** interface will appear.



3. Make any necessary changes and click **OK**.

Note: This procedure only works with certificate templates that issue certificates that sign other certificates, such as **Cross Certification Authority** and **Root Certification Authority**.

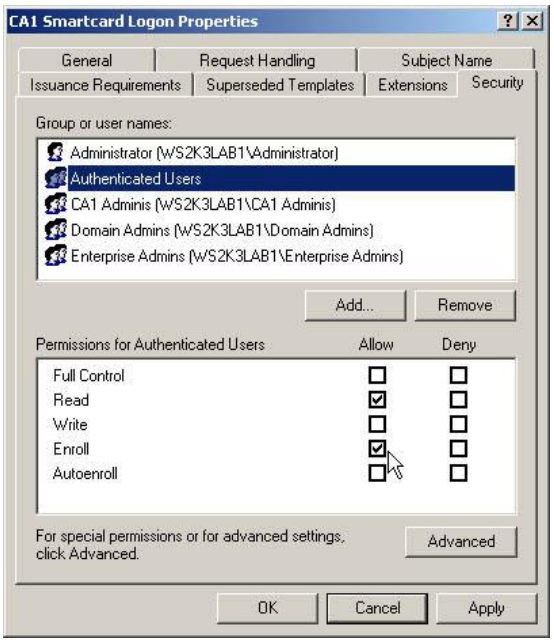
Copyright © 2008 Microsoft Corporation.

All rights reserved.

Security

The Security tab allows CA Administrators to define the permissions, or discretionary access control list (DACL), for a specific certificate template. The permissions that are assigned to the certificate template define which security principals can read, modify, enroll, or auto-enroll for a specific certificate template.

Note: It is recommended that certificate template permissions be assigned only to global groups or universal groups. Because the certificate template objects are stored in the Configuration naming context, the CA Administrator cannot assign permissions using domain local groups. To simplify administration, it is never recommended to assign certificate template permissions to individual user or computer accounts.



The permissions that can be assigned to a certificate template include:

- **Full Control**. This permission allows a security principal to modify all attributes of a certificate template, including the permissions for the certificate template.
- **Read**. This permission allows a security principal to see the certificate template when enrolling for certificates. It is required for a security principal to enroll or auto-enroll a certificate; it is required by the certificate server to find the certificate templates in Active Directory.

Note: It is considered a best practice to keep **Read** permission assignment for the Authenticated Users group. This permission assignment allows all users and computers to view the certificate templates in Active Directory. This includes allowing the CA running under the SYSTEM context of a machine account to view the certificate templates when issuing certificates to users and computers.

- **Write**. This permission allows a security principal to modify the attributes of a certificate template, including the permissions assigned to the certificate template.
- **Enroll**. This permission allows a security principal to enroll for a certificate based on the certificate template. To enroll for a certificate, the security principal must also have **Read** permissions for the certificate template.
- **Autoenroll**. This permission allows a security principal to receive a certificate through the auto-enrollment process. Auto-enrollment permissions require that the user has both **Read** and **Enroll** permissions in addition to the **Autoenroll** permission.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

CA Key Management

Within the TOE, Windows Server 2003 Certificate Server uses a FIPS PUB 140-2 validated HSM. This subsection describes the functions that can be administered through the Certificate Server component.

The HSM selected for use in the Windows Server 2003 Certificate Server is the nCipher nShield HSM (Model nShield F3 UltraSighn PCI – nC4032P-300), which integrates with the Microsoft Windows Server 2003 Certificate Server via the Microsoft CryptoAPI. The nCipher nShield HSM provides advanced key management, key recovery capabilities, and transaction acceleration functionality within a single FIPS PUB 140-2 Level 3 certified hardware module. In this integration the Microsoft Windows Server 2003 Certificate Server, through the CryptoAPI, uses the nCipher nShield HSM to securely perform cryptographic operations.

The benefits of using the nCipher nShield HSM with Microsoft Windows Server 2003 Certificate Server include:

- The use of FIPS 140-2 Level 3 validated hardware,
- Secure storage of CA keys,
- Management of the full key life cycle,
- Acceleration of cryptographic processing, and
- Failover support.

Changing policy settings on the CA

The CA Administrator can configure a number of settings in the default policy and exit modules provided with Certificate Services by using the CA's **Properties** interface.

Specify CA certificate access points in issued certificates

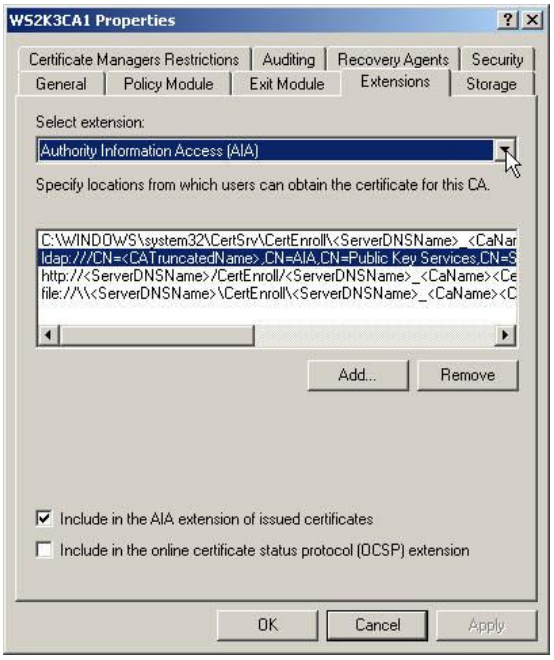
CA Administrators can modify the certificate distribution points that are listed in the **Authority Information Access** extension view, on the **Extensions** tab of the CA **Properties** interface, to ensure that users have convenient access to the certificate for a specified CA. The certificate for the CA is published to the specified certificate distribution points. In addition, the CA writes these certificate distribution points into every certificate that it issues.

To add, remove, or modify certificate access points:

1. Log on to the computer as a CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. In the console tree, right-click the CA node and select **Properties**.
4. On the CA **Properties** interface, select the **Extensions** tab.
5. Select the **Authority Information Access (AIA)** extension from the **Select extension** drop-down menu.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



6. To make changes or additions to the list of CDPs, do one or more of the actions shown in the Table B-13 below.

Table B-13 Procedures for Modifying AIAs

To	Do this
Add a URL that will be published as part of any certificate issued by a CA.	Click **Add**, then type a URL where users can obtain the CA's certificate.
Remove an authority information URL from the list on issued certificates.	Select the URL and then click **Remove**.
Indicate that that you do not want to use a URL as an authority information access point in certificates without removing it from the list.	Clear the **Include in the AIA extension of issued certificates** check box.
Indicate that a URL can now be used as an authority information access point.	Select the **Include in the AIA extension of issued certificates** check box.
Indicate that a URL can now be used for online certificate status protocol (OCSP).	Select the **Include in the online certificate status protocol (OCSP) extension** check box.
Indicate that that you do not want to use a URL for online certificate status protocol (OCSP) in certificates without removing it from the list.	Clear the **Include in the online certificate status protocol (OCSP) extension** check box.

7. Click **Yes** to stop and restart the Certificate Services service.

Certificate revocation list URLs can be HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Lightweight Directory Access Protocol (LDAP), or file addresses. Use the variables shown in Table B-14 when specifying the address of the AIA.

Table B-14 AIA Address Variables

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Variable	Description
CAName	The name of the certification authority.
CAObjectClass	The object class identifier for a certification authority, used when publishing to an LDAP URL.
CATruncatedName	The "sanitized" name of the certification authority, truncated to 32 characters with a hash on the end.
CDPObjectClass	The object class identifier for CRL distribution points, used when publishing to an LDAP URL.
CertificateName	The renewal extension of the certification authority.
ConfigurationContainer	The location of the Configuration container in Active Directory.
CRLNameSuffix	Inserts a name suffix at the end of the file name when publishing a CRL to a file or URL location.
DeltaCRLAllowed	When a delta CRL is published, this replaces the CRLNameSuffix with a separate suffix to distinguish the delta CRL.
ServerDNSName	The Domain Naming System (DNS) name of the certification authority server.
ServerShortName	The NetBIOS name of the certification authority server.

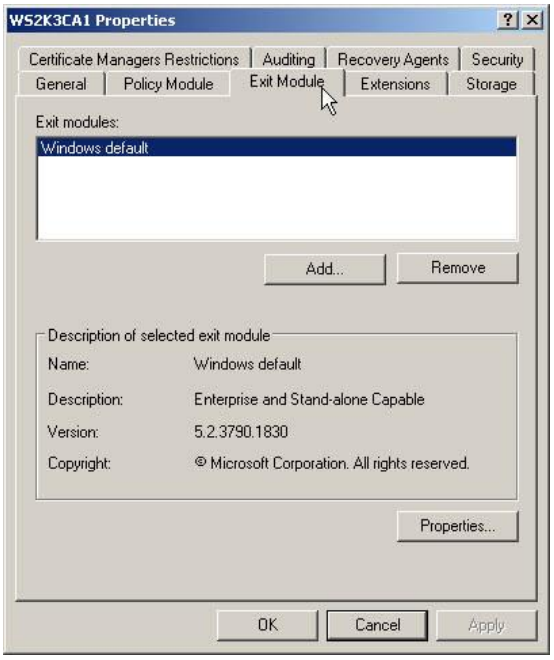
Publish certificates to the file system

No matter what exit modules are installed, certificates are not published unless the publication location is specified in the certificate request. The exit modules enable certificates to be published to the locations specified in certificate requests.

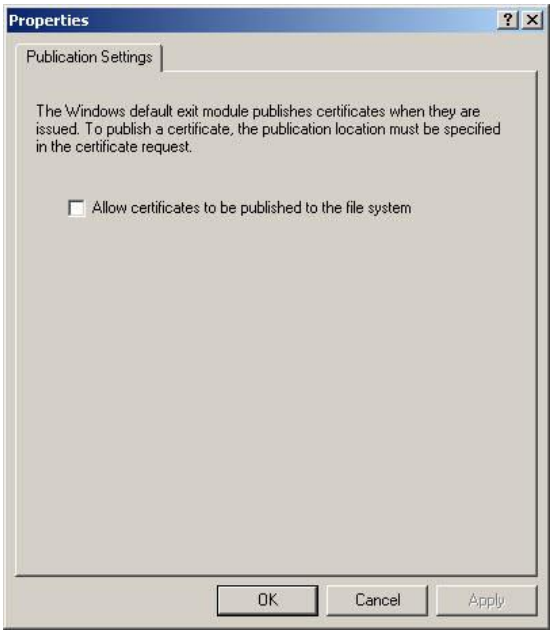
1. Log on to the computer as a CA Administrator.
2. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and select **Certification Authority**.
3. In the console tree, right-click the CA node and select **Properties**.
4. On the CA Properties interface, select the **Exit Module** tab.

Copyright © 2008 Microsoft Corporation.

All rights reserved.



5. Click **Properties** on the **Exit Module** tab. The **Publication Settings** interface will appear.



6. To publish certificates to the file system, select the **Allow certificates to be published to the file system** check box.
7. Stop and restart the CA.

Notes:

- By default, this option is selected for the default stand-alone exit module. To prevent publishing certificates or CRLs to the file system, clear the check box associated with this option. By default, the check box for this option is cleared for the default enterprise exit module. To enable certificates to be published to the file system, select the check box associated with this option.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

- For enterprise CAs, certificates are published to Active Directory by default.

Security-Relevant Events

This subsection describes all types of security-relevant events and what administrator action (if any) to take in order to maintain security. Security-relevant events that may occur during operation of Windows Server 2003 Certificate Server must be adequately defined to allow administrator intervention to maintain secure operation. Security-relevant events are defined as events that signify a security related change in the system or environment. These changes can be categorized as routine or abnormal. The routine events are already addressed in the subsection "Security Functions." For example, the Certificate Server handles a request for a new certificate or for renewing an existing certificate made by a user. Abnormal events are those that do not occur on a regular basis or are a result of limits being reached as set by the administrative staff.

Compromise of Private Key for User, Service or System

Description of event: A user's private key has been compromised.

Security Impact: The compromised private key may be used to gain unauthorized access to resources or to impersonate a security principal. This may occur if the user has stored an unprotected copy of the private key offline and an unauthorized user has gained access to it.

Required Activities: Revoke the security principal's certificate, update the CRL, and have the security principal request a new certificate with a different key.

1. If the compromised certificate is an EFS certificate, have the user decrypt any encrypted data and store it in a safe location that is inaccessible to the network, such as removable media.

   Note: Alternatively the data may be recovered by a Data Recovery Agent (DRA) after the user's certificate is revoked. Procedures for using a DRA to recover a user's encrypted data are provided in the Data Recovery subsection of this document.

2. Revoke the security user's certificate.
3. Update the CRL to make sure the recently revoked certificate is included in the latest CRL.
4. Have the security principal request a new certificate with a different key.
5. If the user previously decrypted and backed up any data, the user may restore the data to the original location and may encrypt it using the new EFS certificate.

   Note: Procedures for revoking a certificate are provided in the Revoking a certificate subsection. Procedures for updating the CRL are provided in the Publishing a CRL before the next scheduled publish period subsection. Procedures for requesting a new user certificate are provided in the "Certificate request procedures" subsection of the *Windows XP Professional with SP2 User's Guide, Version 3.0*.

User Leaves Organization

Description of event: A user leaves the organization and no longer requires access to network resources.

Copyright © 2008 Microsoft Corporation.

All rights reserved.

Security Impact: If the user's certificates are not revoked, the user may retain access to resources within the organization or secured resources that may be accessible through public networks. For example, the user may retain access to the organization's secured Web site.

Required Activities:

1. Verify that the user has not encrypted any essential files or directories. If so, make sure they can be decrypted before deleting the user account.

   Warning: If the administrator changes the password for a local user account, the user's access to any previously encrypted files will be lost. Therefore, changing a user account's password to gain access to encrypted data will not work. Make sure there is a DRA or that an alternate account also has access to the encrypted files before deleting the user account. See the Data Recovery subsection of this document.

2. Disable or delete the user's network account.
3. Revoke the user's certificates.
4. Publish a new CRL.

   Note: Procedures for disabling or deleting user accounts are provided in the Creating and Maintaining User and Group Accounts subsection of this document. Procedures for revoking a certificate are provided in the Revoking a certificate subsection. Procedures for updating the CRL are provided in the Publishing a CRL before the next scheduled publish period subsection.

Audit Certification Authority Management Activities

Description of event: Identify and monitor security-relevant events related to the management of the Certification Authority by requiring auditors to review audit logs on a regular basis.

Security Impact: Monitoring audit logs on a regular basis may be useful for timely identification of unauthorized access and modification attempts, misuse of administrative privileges, or to identify and troubleshoot problems related to the function and maintenance of the CA.

Required Activities:

1. Enable auditing of CA management activities.

   Note: Procedures for enabling audit of CA management activities are provided in the Configuring auditing of CA administrative actions subsection.

2. Review audit logs. Filter audit logs, if necessary, to view CA specific activities.

   Note: Procedures for viewing and filtering the audit logs are provided in the Viewing CA administrative audit events in the system security log subsection.

User Must Be Removed from a CA Management Role

Description of event: A user is no longer authorized to have access privileges related to a CA management role.

Security Impact: The user may retain the ability to perform "unauthorized" CA management actions on the CA if the privileges or permissions associated with the management role are not removed.

Required Activities:

Copyright © 2008 Microsoft Corporation.

All rights reserved.

1. CA management roles are assigned through membership in one of the four designated CA management role groups. To remove a user's CA management role privileges, remove the user's account from the designated management role group. Prior to removing the user's CA management rights, ensure that the right has been granted to another designated user account assigned to take over that CA management role.
2. If the user's account is not to be disabled or deleted, ensure the account is a member of an appropriate user group within the organization, such as Domain Users. This ensures that user level access rights are retained.

Note: Group accounts defined for CA management roles, and their associated privileges and permissions are defined in Tables A-3 and A-4 of Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide. Procedures for removing or adding user accounts to groups are provided in the Creating and Maintaining User and Group Accounts subsection of this document.

A New User Must Be Granted a CA Management Role

Description of event: A user has recently been assigned to a specific CA management role.

Security Impact: Within the TOE, Windows Server 2003 Certificate Server requires the designation of four CA management roles: CA Administrator, CA Manager, CA Auditor, and CA Backup Operator. Due to role separation requirements, a single user account cannot perform multiple role functions. Therefore, it is important to assign different user accounts to each of the specific CA management roles.

Required Activities:

1. Make the user a member of the domain group that is designated for the desired CA management role.

Note: Group accounts defined for CA management roles, and their associated privileges and permissions are defined in Tables A-3 and A-4 of Appendix A, Windows Server 2003 Certificate Server Security Configuration Guide. Procedures for adding user accounts to groups are provided in the Creating and Maintaining User and Group Accounts subsection of this document.

2. Ensure the user is not assigned to more than one CA management role. If the user is assigned to more than one role, the role separation restrictions configured on the CA will not allow the account to perform any CA management activity assigned by a role

Copyright © 2008 Microsoft Corporation.

All rights reserved.